Haaga-Helia
ammattikorkeakoulu Oy

Esineiden Internet standardit ja protokollat

Thomas Mata

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2015

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

13.5.2015

Tekijä(t)
Thomas Mata

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Esineiden Internet standardit ja protokollat

Sivu- ja liitesivumäärä
43

Opinnäytetyön otsikko englanniksi
Internet of Things standards and protocols

Tässä opinnäytetyössä tutustutaan esineiden Internet –maailmaan ja sitä sivuaviin aiheisiin, kuten tiedonvälitykseen ja yhteentoimivuuteen. Esineiden Internet on ilmiönä kiinnostava ja tulee mullistamaan lähitulevaisuudessa ihmisten ja laitteiden välistä vuorovaikutusta.

Projektin ensimmäisessä puoliskossa käydään läpi mitä IoT –protokollilla tarkoitetaan ja selvitetään miten erilaiset ratkaisut saadaan toimimaan näiden avulla. Seuraava esineiden Internetin kehityksen vaihe on saada älykkäät laitteet yhdistettyä ja kommunikoimaan keskenään keräten näin arvokasta dataa ympäristöstä, laitteista, koneista ja ihmisistä. Oleellisena osana esineiden Internetiä toimivat standardit. Ilman näitä kehitystä ei voisi tapahtua, koska koko tuntemamme Internet toimii juuri standardien pohjalta ja tämä tulee myös mahdollistamaan laitteiden välisen kommunikoinnin. Monet eri tahot pyrkivät IoT –markkinoille ja tähän päivään mennessä monet yritykset ovat lyöneet voimansa yhteen liittyen organisaatioihin, kuten OIC, AllSeen Alliance ja Thread Group, jotka kehittävät yhteistyössä avoimen standardin IoT –ratkaisuja.

Opinnäytetyön viimeinen osio käsittelee IoT –laitteiden virranhallintaratkaisuja. Työssä tutkitaan miten IoT –esineet ja sensorit tulevat toimimaan kuukausia tai vuosia ilman virtalähteen lataamista. Kehityksessä on keskityttävä mahdollisimman suureen energiatehokkuuteen, mutta samalla muistaa kustannustehokkuus. Työn lopussa käsitellään IoT:hen liittyviä tietoturva-asioita. Laitteiden välisessä kommunikoinnissa kertyy valtava määrä dataa ja tämä täytyy myös varastoida johonkin. Arvokas data tulee houkuttelemaan hakkereita toimimaan.

Projektin tuloksena syntyy kirjallisuuskatsaus IoT –maailmasta, sen nykytilasta ja tulevaisuuden näkymistä. Näkemykset eroavat siinä, että tuleeko IoT vasta 10 tai 15 vuoden päästä vai onko ilmiö jo ympärillämme. Tällä hetkellä voi jo hankkia useita älylaitteita, jotka toimivat tässä projektissa selvitettyjen ratkaisujen pohjalta.

Asiasanat
Esineiden Internet (IoT), sensorit, laitteet, esineet, standardit, protokollat

HAAGA-HELIA
University of Applied Sciences

Abstract

13.5.2015

Author(s)
Thomas Mata

Degree programme
Business Information Technology

Report/thesis title
Internet of Things standards and protocols

Number of pages and appendix pages
43

The objective of this thesis is to determine what is the Internet of things (IoT). In addition, the aim is also to explore the related topics, such as communication and interoperability. The phenomenon of the Internet of things is interesting and is expected to change the interaction between people and devices in the near future.

The first half of the project examines what the IoT –protocols mean and explains how different solutions work for them. The next step of the development of the IoT is to get smart devices connected and communicating with each other thus collecting valuable data about the environment, devices, machines and people. An integral part of the IoT is the operating standards. The Internet itself operates on standards, and standards will enable things to communicate with each other. Without them, this development cannot occur. Many different actors aim at the market and to date many companies have teamed up to form organizations, such as OIC, AllSeen Alliance and the Thread Group that will cooperatively develop the open standard IoT –solutions.

The last section of the thesis deals with the power management solutions on IoT –devices. The study examines how the IoT –devices and sensors are going to work for months or years without recharging. Development must focus on the maximum energy efficiency, but at the same time considering cost efficiency factor. The last part of this thesis deals with IoT –related security issues. The huge amount of data has been accumulated via communication between devices, and this also needs to be stored safely. Valuable data will attract hackers.

The outcome of the study is an inclusive review of IoT, its current state and future prospects. At this very moment there are a number of smart devices that work on many solutions discovered through this project.

Keywords
Internet of Things (IoT), sensors, devices, things, standards, protocols

Sisällys

1 Johdanto

Esineiden Internet on ilmiönä kiinnostava, koska se tulee jo lähitulevaisuudessa mullistamaan ihmisten ja laitteiden välistä vuorovaikutusta. Teollisuuden arvioidaan synnyttävän liiketoimintaa tuhansien miljardien arvosta. Buumi on tällä hetkellä kovimmillaan ja yritykset haluavat pysyä ajan hermoilla ja taistelevat markkinaosuuksista. Aihe on enenevässä määrin esille sosiaalisessa mediassa puhuttaessa seuraavasta teknologisesta kehitysvaiheesta.

Työn tarkoituksena on selvittää millaisia esineiden Internet (IoT) –ratkaisuja tällä hetkellä on tarjolla sekä mitä haasteita näiden ratkaisujen toteuttaminen tuottaa. Tutkimuksessa käydään läpi jatkuvasti kasvavalle alalle kehitettäviä IoT –protokollia ja standardeja, joissa laitteet vaativat jatkuvasti kehittyneempiä ja laajempia ratkaisuvaihtoehtoja. Lisäksi selvitetään miten esineiden Internet toimii eri standardien pohjalla ja miten ne mahdollistavat laitteiden välisen kommunikoinnin.

Yksi tällä hetkellä tutkituista toimialoista on koneiden välinen kommunikointi (M2M) ja langattoman anturiverkko (WSN) –ratkaisujen integrointi toisten Internet –palvelujen kanssa käyttäen olemassa olevia Internet –protokollia. IoT on tuonut mahdollisuuden toimijoille kehittää ja laajentaa protokollien käyttötarkoituksia, joilla saataisiin toimivammat ratkaisut tiedonsiirtotekniikoille. Ensin täytyy ymmärtää sovellusten tarkoitus liittyen käyttöönottoon, hallintaan, tukimahdollisuuksiin ja parhaisiin toteutuksiin, jotta voidaan valita optimaalisin protokolla käytettäväksi järjestelmille. IoT –standardit otettiin käyttöön, jotta voitaisiin hallita neljää osa-aluetta: liitettävyys, yhteentoimivuus, yksityisyys ja turvallisuus. Miten markkinoilla kamppailevat standardisointi -ryhmittymät tulevat toimimaan näiden IoT -osa-alueiden suhteen?

Ajatusmaailma esineiden Internetin tulevaisuudesta näyttäisi olevan merkittävä, mutta riittävätkö resurssit ylläpitämään tätä valtavaa verkkokokonaisuutta? Yhtenä mahdollisena hidastuksena nopeaan kehitykseen tulee olemaan toimijoiden halu kehittää omia ratkaisuja sen sijaan, että rakennettaisiin yhtenäistä IoT –tekniikkaa. Toisena hidasteena tulee olemaan päätelaitteiden virranhallintaratkaisut. Laitteiden on tarkoitus toimia itsenäisesti vähintäänkin kuukausia ja jopa vuosia ilman ylimääräistä virtalähteen lataamista. Tutkimuksessa käydään läpi miten virransyöttö on toteutettu IoT –laitteissa.

Viimeisessä osassa tutkimusta selvitetään kulkevatko teknologia ja turvallisuus samalla viivalla. Pysyvätkö kaikki laitteiden ja esineiden välinen tiedonsiirto turvassa epäystävällisiltä tahoilta? Kaikki mikä tulee olemaan yhteydessä IoT –laitteisiin, kuten älypuhelimet,

erilaiset mittarit ja kodinkoneet, tulevat olemaan erittäin houkutteleva hyökkäyksen kohde. Kuten älypuhelinten kehityksen aikana, ovat tietoturvaongelmat usein käyttäjän kannalta huonosti tiedostettu tosiasia, jota ei oteta tarpeeksi vakavasti.

1.1 Käsitteet

ACK (Acknowledgement): signaali, joka kulkee kommunikoinnin yhteydessä määritellen vastauksen.

Hub-and-Spoke: mallissa järjestelmäintegraatio toimii keskistettynä pisteenä, jossa data-integraatio tapahtuu.

M2M (Machine-to-Machine): kahden erillisen laitteen välistä tiedonsiirto ja kommunikointi.

M2P (Machine-to-People): laitteen ja ihmisen välinen tiedonsiirto ja kommunikointi.

NAT (Network Address Translation): osoitteenmuunnos.

Peer-to-Peer: vertaisverkko, jossa ei ole kiinteitä palvelimia ja asiakkaita.

P2P (People-to-People): ihmisten välinen tiedonsiirto ja kommunikointi.

QoS (Quality-of-Service): tietoliikenteen luokittelu ja priorisointi.

REST (Representational State Transfer): HTTP –protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen.

RFC (Request for comments): IETF –organisaation julkaisemia Internetiä koskevia standardeja.

SSM (Single Source Multicasting): luotettava yhteydellinen viestipohjainen kuljetuskerroksen protokolla.

UPD (User Datagram Protocol): yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron.

WEP (Wired Equivalent Privacy): työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaaman kehitetty salausmenetelmä.

WPA (WiFi Protected Access): välivaiheen tietoturvatekniikka, joka kehitettiin WEP –salauksen ongelmien paljastuttua.

WPA2: langattomien 802.11 –verkkojen viimeisin tietoturvastandardi.

WSN (Wireless Sensor Network): sensoriverkko, joka tarkkailee ympäristön olosuhteita, kuten lämpötilaa, ääniä ja ilmanpainetta.

1.2 Lyhenteet

AMQP: Advanced Message Queuing Protocol

CoAP: Constrained Application Protocol

DDS: Data Distribution Service

DTLS: Datagram Transport Layer Security

HTTP: Hypertext Transfer Protocol

IoT: Internet of Things (Esineiden Internet)

MQTT: Message Queue Telemetry Transport

XMPP: The Extensible Messaging and Presence Protocol

6LoWPAN: IPv6 ja Low-power Wireless Personal Area Networks -yhdistelmä

2 Esineiden Internet

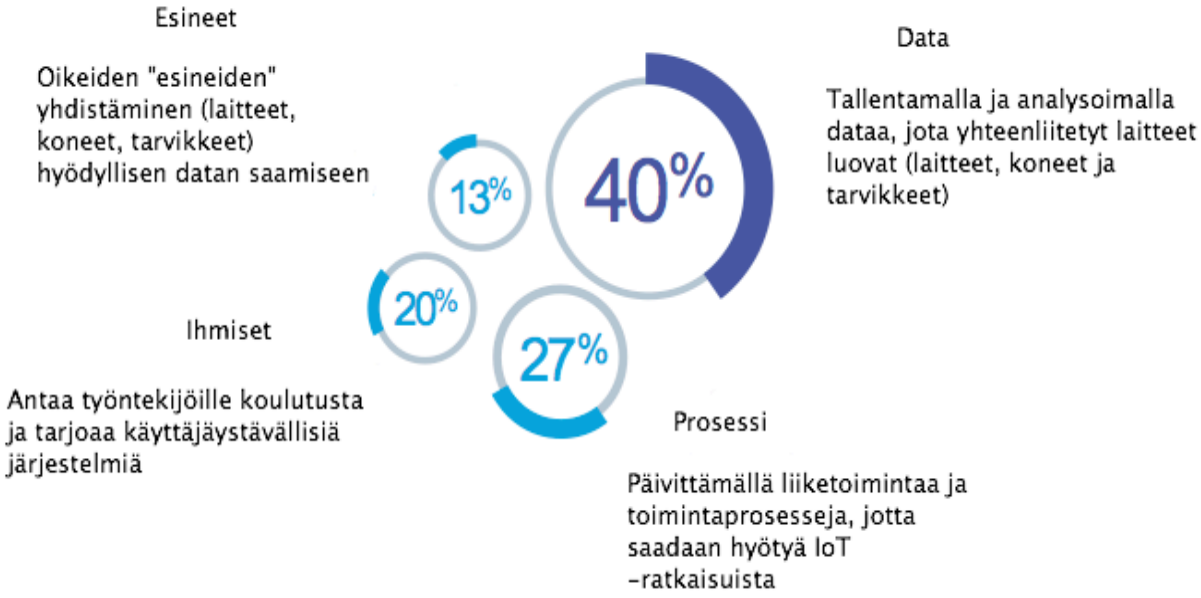
Esineiden Internet on nopeasti kasvava puheenaihe maailmassa. Kyseessä on seuraavan sukupolven Internet, joka yhdistää ihmisten lisäksi myös fyysiset laitteet keskenään. Laitteet ovat yhteydessä toisiinsa, keskustelevat keskenään sekä keräävät suuren määrän tietoa. Laitteiden keskustellessa keskenään ne luovat, analysoivat ja jakavat tämän tiedon tarkoituksenaan helpottaa ihmisten jokapäiväistä työntekoa ja elämää. (Intel 2014.)

Internet of Things –termin otti esiin ensimmäisenä Kevin Ashton vuonna 1999. Ashtonin mukaan tietokoneet ja Internet ovat lähes täysin riippuvaisia ihmisistä. Alun perin karkean arvion mukaan noin 50 petabittiä (1 petabitti on 1024 terabittiä) tiedosta Internetiin on kirjoitettu, painettu, nauhoitettu tai skannattu. Ongelmana on ihmisen rajattu aika, huomio ja tarkkuus, jolloin tiedon keruu ympäröivästä maailmasta ei ole riittävää. Ashtonin mukaan tarvitsemme laitteita, jotka keskustelevat keskenään käyttäen keräämäänsä tietoa ilman ihmisen apua. Tarkoituksena on kehittää laitteet näkemään ympäröivä maailma sensoreiden avulla. Tällöin me voisimme seurata milloin laite tarvitsisi huoltoa tai vaihdon uuteen. (Ashton 2009, 1.)

Esineiden Internetissä fyysinen maailma yhdistyy Internetiin. Mitä sitten tarkoitetaan termillä ’Things’ (esineet)? Käytännössä kaikki mitä näemme arkipäiväisessä elämässä, kuten laitteet, rakennukset, autot, koneet tai eläimet voivat olla osa IoT:ta. Saadaksemme jonkin objekti liittymään verkkoon, se täytyy identifioida antamalla sille yksilöllinen tunniste eli oma IP -osoite. Oman tunnisteen avulla objektille saadaan yhdistettävyys mahdollisuus. Objektiin on liitettävä sensoreita, jotka keräävät ja mittaavat ympäristöään sekä tallentavat ja välittävät tapahtumia tietoliikenneyhteyden välityksellä edelleen tarvittuihin kohteisiin. Sensoriin voidaan asentaa sirukortti, joka kykenee datan välitykseen ja vastaanottoon. (Barrett 2012.)

Käsitteenä Internet of Things (IoT) eroaa Internet of Everything:stä (IoE). Cisco otti ensimmäisenä esiin käsitteen Internet of Everything, jolla tarkoitetaan käytännössä kaikkien (ihmiset, data, esineet ja prosessit) yhdistymistä. Tavoitteena on saada verkostoituminen oleellisemmaksi ja arvokkaammaksi, jotta voitaisiin luoda uusia rikkaampia kokemuksia ja ennennäkemättömiä mahdollisuuksia liiketoimintaan, yksilöille ja valtioille. Ciscon näkemyksen mukaan IoE, jonka neljä pääpilaria ovat ihmiset, data, esineet ja prosessi, rakentuvat IoT:n päälle, joka koostuu esineistä/asioista. Lisäten esineiden Internetin kasvuprosessin Internet of Everything:iin saadaan kehittyneemmät tulokset liiketoiminnalle ja teollisuudelle sekä ennen kaikkea tavan parantamaan ihmisten elämää. (Evans 2013, 1.)

Kuten seuraavasta kuvasta (kuva 1) käy ilmi, yksi oleellisimmista asioista IoT:ssä on se, että kyse ei ole loppujen lopuksi itse laitteista ja esineistä vaan niiden keräämästä datasta.



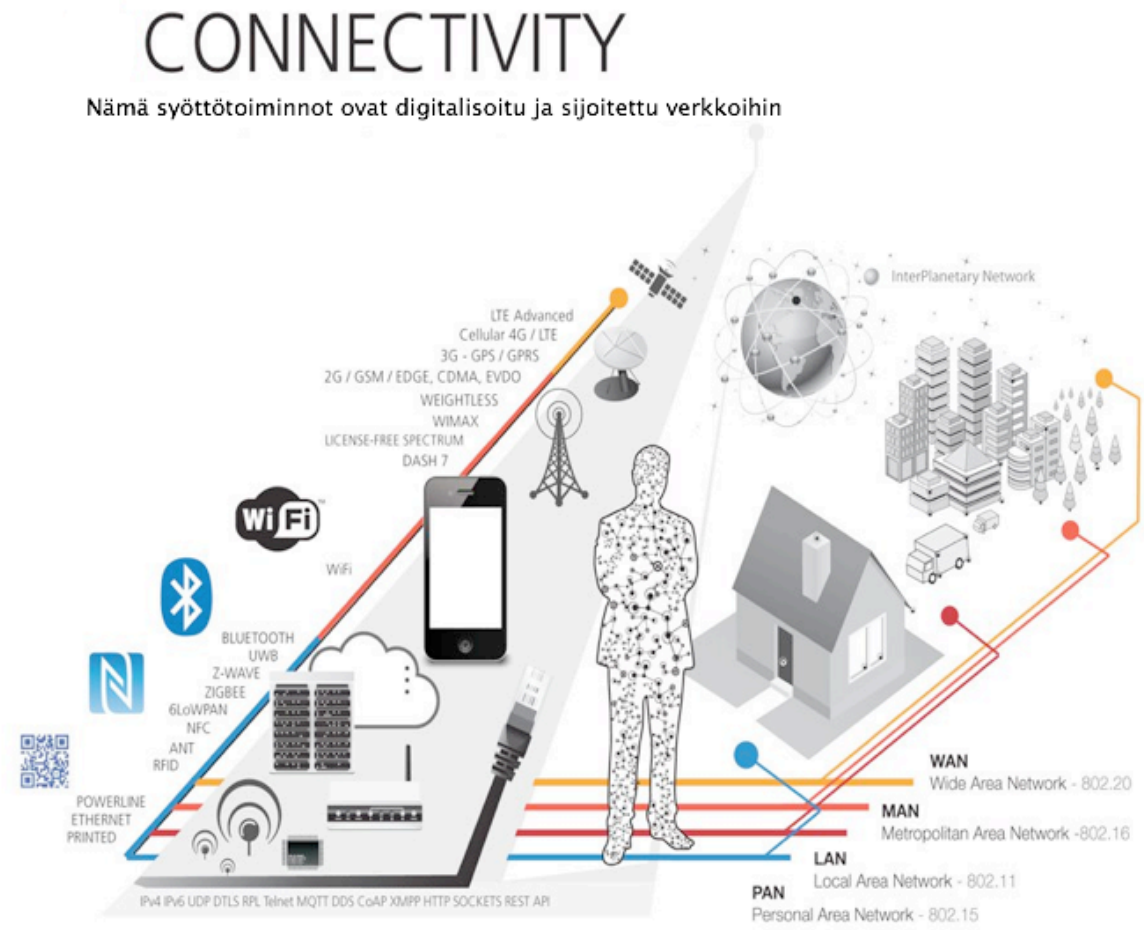
Kuva 1. IoT osa-alueet (Cisco)

IoT –maailman ratkaisut koostuvat usein pienitehoisista laitteista ja niiden kanssa paikallisella radio- tai johdinverkolla keskustelevasta Internetiin kytketystä laitteesta sekä verkossa sijaitsevasta palvelusta. Rajoittamalla laitteiden kokoa, energiankulutusta ja hintaa voidaan kytkettyjä laitteita tuoda uusiin käyttökohteisiin. Edellä mainitut tekijät ovat edesauttaneet luomaan kevyitä protokolla- ja verkkoratkaisuja, joiden avulla käyttäjille voidaan rajoitteista huolimatta tarjota ratkaisuja, joita aikaisemmin ei voitu edes kuvitella toteutettaviksi. (Syrjälahti 2015, 1.)

IoT –ekosysteemiin kuuluu laitteita älykkäistä kodinkoneista (jääkaapeista, leivänpaahtimista ja ilmastointijärjestelmistä) ja autoista päälle puettaviin laitteisiin ja kaikkeen siltä väliltä. Vaikka nämä eroavat menetelmiltään ja käytöltään, kaikki laitteet hyödyntävät neljää kriittistä toiminnallisuutta: aistimista, keräämistä, liitettävyyttä ja datankäsittelyä. Oleellista on se, että IoT –laite aistii jotain. Näin laite kerää dataa siitä mitä se aistii. Lopulta kerätty data välitetään verkon välityksellä toiselle laitteelle tai jonnekin muualle prosessoitavaksi ja analysoitavaksi. (Lattice 2015, 3.)

2.1 Verkot ja niiden kattavuusalueet

Alla olevan kuvan (kuva 2) mukaisesti verkkojen kattavuusalueet voidaan jakaa neljään kategoriaan. Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN) ja Wide Area Network (WAN).



Kuva 2. Verkon kattavuusalueet ja applikaatioita eri verkoissa (Postcapes 2015, 2).

PAN -verkko on henkilökohtainen verkko. Yleisin langaton laite PAN:ssa on älypuhelin, joka on yhteydessä Bluetooth:in kautta erilaisiin oheislaitteisiin kuten kuulokkeisiin, kelloon ja mikrofoniin. PAN:it ovat yleensä langattomia ja näiden kantama on metreistä kymmeniin metreihin. Langattomien PAN –laitteiden akkuvaraus on yleensä suhteellisen pieni. (Reiter 2014, 4.)

LAN on joko langaton tai langallinen verkko tai näiden yhdistelmä. Kantavuusalue on yleensä noin 100 metriä. Tyypillisin ja eniten käytössä oleva esimerkki on kotiverkko, josta jaetaan yhteys mm. tietokoneisiin, älypuhelimiin ja televisioihin. (Reiter 2014, 4.)

Voimakastasoinen, mutta vähemmän tiedonsiirtoa käyttää langaton MAN, joka kattaa isomman alueen kuin LAN, mutta pienemmän kuin WAN. Esimerkiksi kaupunki tai useamman LANin yhdistelmä kuuluvat MAN -verkkoon. Viimeisimpänä trendinä tuli langattoman rakennelman MAN. (Rouse 2015, 1.)

WAN on kattavin verkko ja muun muassa Internet mielletään WANiksi, joka koostuu sekä langallisista että langattomista yhteyksistä (Reiter 2014, 4-5).

2.2 IoT -sensorit ja laitteet

Esineiden Internetin ydin on siinä, että laitteita kytketään toisiinsa sensoreiden avulla niin, että näiden tuottama informaatio hyödyntää ihmistä. Laitteet liitetään verkkoon ja ne tuottavat tietoa, joka pitää analysoida reaaliajassa. Tehokkain tapa tähän on käyttää pilvipalveluita. Tärkeää on varmistaa tiedontallennus ja tietoturva, kuten kaikessa muussakin uudessa tekniikassa. (Schneider 2014, 2.)

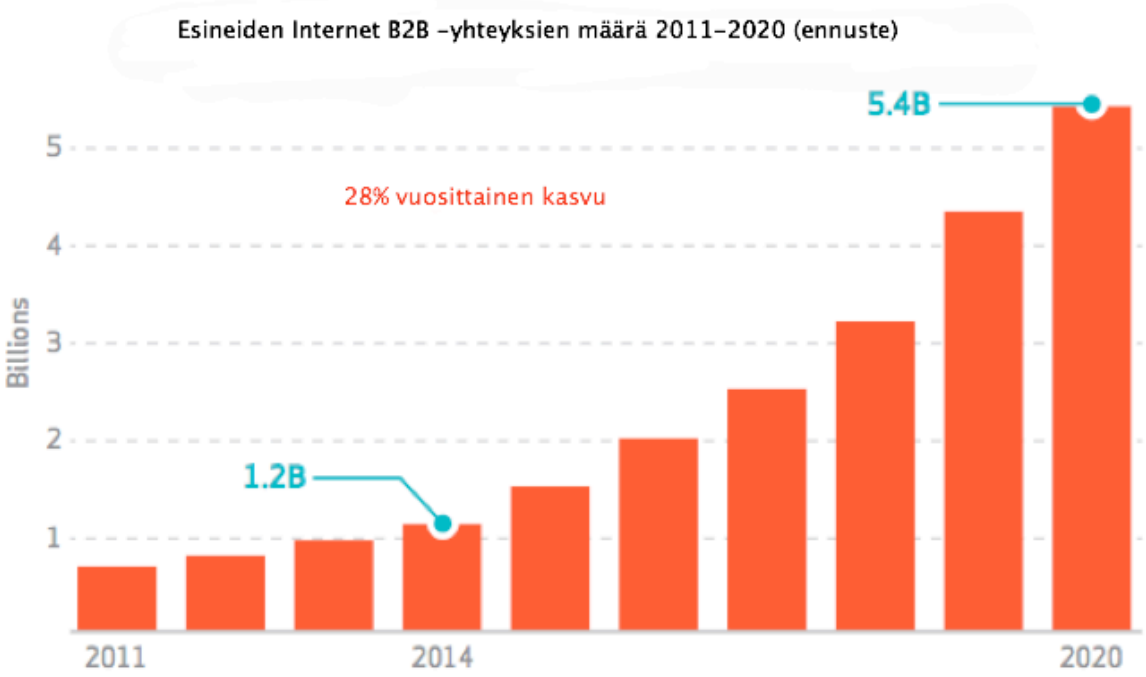
IoT:n ”esineet” voidaan määritellä sisäisiksi laitteiksi, jotka ottavat vastaan ja lähettävät informaatiota verkossa. Nämä laitteet pohjautuvat mikrokontrollereihin, jotka käyttävät ohjelmistoja rajoitetuilla resursseilla. (Schneider 2014, 2.)

IoT antaa uuden tavan ajatella, kun kyseessä on meitä ympäröivät laitteet ja ympäristö. Laitteiden kerätessä jatkuvaa dataa sensoreiden avulla, niin esimerkiksi omasta älypuhelimesta tulee jatkuvasti ympäristöä mittaava laite. Tästä esimerkkeinä voisivat toimia muun muassa sydänmonitori puhelimessa, joka kykenee varoittamaan omistajaa tai omaisia etukäteen vaarasta tai hakukoneiden paranneltu versio, jossa voitaisiin Internetiä koskevien tietojen sijaan hakea tietoa kadonneista kotiavaimista tai missä lapset ovat. Kun tiedetään mitä laitteet tekevät ja mitä ne tuntevat, voidaan näitä entistä tehokkaammin kontrolloida ja hyödyntää. Jo yli puolet maailman väestöstä asuu tällä hetkellä kaupungeissa ja näistä on tärkeä saada paremmin valvottu kokonaisuus sensoreiden avulla, jotta säästettäisiin huomattava määrä energiaa. (Barrett 2012.)

2.3 IoT -kommunikointi

Kaikki IoT -laitteet eivät ole suoraan yhteydessä Internetiin. Osa laitteista, kuten sensorit, kommunikoivat keskenään esimerkiksi paikallisessa verkossa. Näiden keräämä data välittyy paikallisessa verkossa olevaan päätelaitteeseen tai pilvipalveluun. Maailmassa on noin 50 biljoonaa älylaitetta ja IoT:n haasteena ja mahdollisuutena on yhdistää nämä laitteet tavalla, josta on meille todellista hyötyä. IoT tulee yleisten arvioiden mukaan (Kuva 3) yhdistämään kymmenen kertaa enemmän kuin aikanaan mobiililaitteiden luoma vallan-

kumous. Missä nämä kaikki laitteet ovat? Kaikki nämä ovat jo todellisuudessa osa jokaisen elämää. Nykyajan autot käyttävät yli 100 erilaista prosessoria tai ohjelmistoa. Älylaitteet leviävät eri teollisuuksiin, sairaaloihin, koteihin ja julkiseen liikenteeseen. Toistaiseksi nämä systeemit ovat heikosti yhdistetty älylaitteisiin, mutta se tulee lähitulevaisuudessa muuttumaan. (Schneider 2013, 2.)



Kuva 3. Tulevaisuuden kasvuennuste IoT -yhteyksille, ABI Research (Verizon 2015, 5).

3 Protokollat ja IoT

Viimeaikainen kehitys liityntätekniikoissa on ollut vauhdikasta, kun puhutaan älylaitteiden toiminnasta. Koska vauhti ja laatu näissä tekniikoissa kasvaa nopeasti voi olla vaikea saada erilaiset ratkaisut toimimaan saumattomasti yhteen esineiden Internetissä. (Sutaria & Govindachari 2013, 1.)

Meneillään on trendi, jossa integroidaan machine-to-machine (M2M) ja langaton anturiverkko (WSN) –ratkaisuja toisten Internet –palvelujen kanssa käyttäen olemassa olevia Internet -protokollia. Suurimmat haasteet, jotka IoT –toteutukset kohtaavat ovat sekä vähän virtaa käyttävät laitteet, joiden on tarkoitus toimia kuukausista vuosiin ilman virranlatausta että tiuha tiedonsiirto verkoissa. (Sutaria & Govindachari 2013, 1-2.)

Jatkuvasti luodaan uusia IoT –protokollapinoja ja avoimia standardeja. Olemassa on langattomia protokollia, kuten ZigBee, RIFD, Bluetooth ja BACnet ja uuden sukupolven protokollia kuten 802.15.4e, 6LoWPAN, RPL ja CoAP, joilla pyritään yhdistämään langaton sensoriverkko ja Internet. IoT on kunnianhimoinen ajatusmalli, jossa yhdistettyjen laitteiden määrä on jatkuvassa kasvussa. Tämän hallitseminen vaatii uusia ja tehokkaampia teknologioita. Meneillään oleva standardisointi, jossa Internet protokollat saadaan WSN –pohjaiseen esineiden Internetiin on herännyt toivoa maailmanlaajuisesta yhdistymisestä kuljetuskerroksen (Transport layer) ja sen alapuolella olevien kerrosten osalta. (Sutaria & Govindachari 2013, 2.)

Internet on omassa suuruusluokassaan onnistunut hyvin antamaan valinnanvaraa standardeissa kuten HTTP, SMTP ja SSH, eikä sen tarvitse käsitellä ongelmia tai rajoituksia, kuten virran- tai datanmenetyksiä. Äly-, vähävirtaisilla- ja WSN –laiteilla, joilla halutaan ottaa yhteys Internetiin tulevat kärsimään kyseessä olevista rajoitteista. (Sutaria & Govindachari 2013, 2.)

3.1 IPv4 ja IPv6

Kommunikoidakseen Internetin kautta esineet tarvitset IP –osoitteen, mutta maailmassa ei tule riittämään tarpeeksi näitä nykyisellä IPv4 -protokollalla. Ratkaisuksi luotiin vuonna 1998 julkaistu IPv6, jonka oleellisin kehitys on osoitteiden laajentaminen 32 bittisistä 128 bittisiksi. Se tarkoittaa, että mahdollisia osoitteita on noin 50 000 000 000 000 000 000 000 000 000 000 jokaista maailman asukasta kohti. Lisäksi IPv6 omaa automaattisen asetuksen: tilaton autokonfiguraatio, joka korjaa IPv4:n puutteita ja konfiguroi IP -laitteella osoitteen ja muut asetukset ilman, että käyttäjän tarvitsee tehdä laitteelle mitään muuta kuin

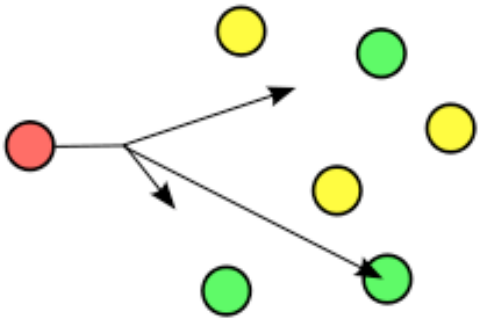
kytkeä se verkkoon. Automaattisessa määrittelyssä kone saa reitittimeltä verkon osoitteen ja muut asetukset. (Rouse 2015, 1-2.)

IPv6 tuo monia välttämättömiä kehitysaskelia, kuten SSM (Single Source Multicasting), joka on tehokas ja skaalautuva tapa lähettää videolähetettä Internetissä monille vastaanottajille. IPv4:n rajallisen osoiteavaruuden vuoksi jouduttiin ratkaisemaan yllättävä laajennus: NAT (Network Address Translation), joka mahdollistaa useiden käyttäjien ja laitteiden IP –osoitteen jakamisen. IPSec on Internetin tietoturva –arkkitehtuuri suojaten yhteyksiä väärinkäytöksiltä ja salakuunteluilta. Laajuuden vuoksi IPv6 mahdollistaa Internetin liitettävyyden mihin tahansa laitteeseen ja palveluun. Kokeiden avulla on näytetty toteen IPv6 onnistuneen käytön sensoreilla älyrakennuksissa- ja kaupungeissa. Mobile IPv6 mahdollistaa Internet –laitteiden verkosta toiseen liikkumisen ilman, että yhteyden katkeavat. IPv6 on suunniteltu myös mahdollistamaan oman älylaitteiden verkon luomisen tai yhdistämisen muuan maailman kanssa. IPv6 pystyy tarjoamaan päätelaitteille useita osoitteita ja parempia reititysmenetelmiä kuin IPv4. (Iot6.eu 2014, 1.)

IPv6:ssa multicast on toteutettu monipuolisemmin kuin IPv4:ssä. FF –alkavat osoitteet ovat kaikki multicast –osoitteita, joten näitä on valtava määrä. Näillä osoitteilla voi olla myös erikokoisia alueita. Osoite voi olla koneen sisäinen, verkkokohtainen, toimialuekohtainen, yrityskohtainen tai koko Internetin alueella toimiva. (Merilinna, 57.)

Broadcast –toiminta on korvattu multicast –osoitteella FF0x::1, jossa x:n arvo riippuu siitä, miten laajalle alueelle viesti halutaan lähettää. FF02::1 vastaa IPv4 broadcast –osoitetta. (Merilinna, 57.)

IPv6 sisältää myös uuden toiminnan nimeltä anycast (Kuva 4), jossa joukko koneita muodostaa ryhmän. Siinä joukko muodostaa ryhmän ja anycast –viestin lähettäessä reitittimet lähettävät viestin lähimmälle ryhmän jäsenelle. Tämä helpottaa esimerkiksi maakohtaisten palvelimien käyttöä. Anycast –ryhmä ei tarvitse erityistä määrittelyä, vaan reitittimet muodostavat automaattisen anycast –ryhmän, jos usealle koneelle antaa saman IPv6 –osoitteen. (Merilinna, 57.)



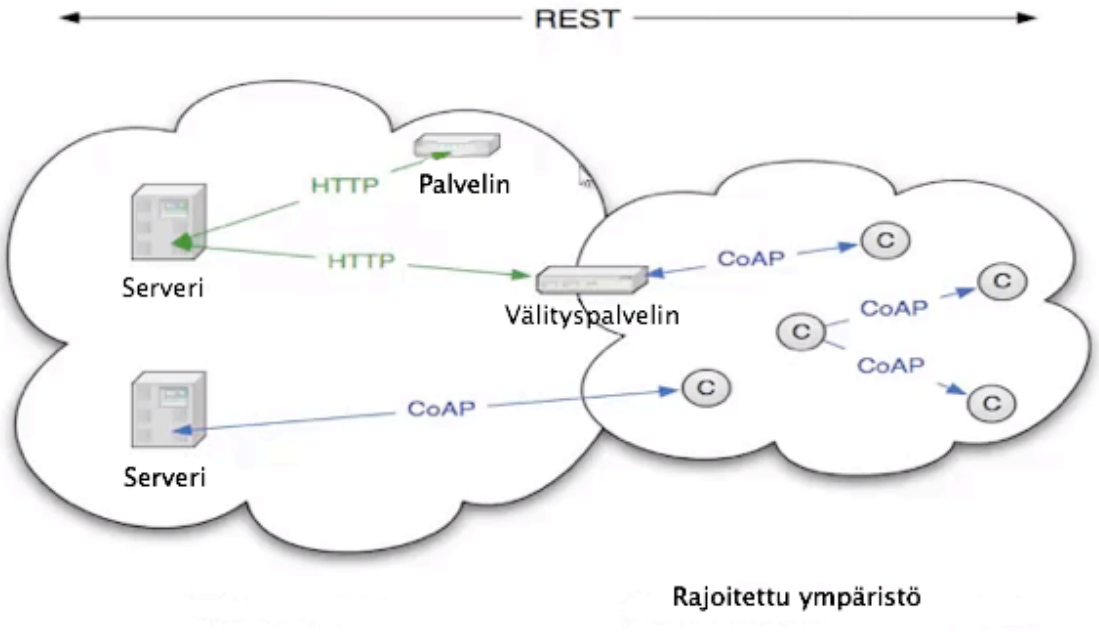
Kuva 4. Anycast.

IoT –maailman ja IPv6 –maailman yhdistäjänä on 6LoWPAN –teknologia, jonka kehittämisessä merkittävässä roolissa on ollut suomalainen Sensinode. Kuten kappaleessa 5.4 tarkemmin käydään läpi, 6LoWPAN –teknologian ideana on käyttää paikallisessa pienen tehon- ja kaistankäytön verkossa kevyttä 6LoWPAN –protokollaa. Tämä muunnetaan täydeksi IPv6 –protokollaksi gateway –laitteessa. Tällä tavoin IoT –laitteet pystyvät helpommin kytkeytymään IPv6 –avaruuden osiksi. (Syrjälahti 2015, 3.)

3.2 CoAP

CoAP (Constrained Application Protocol), jota kutsutaan myös The Web Of Things –protokollaksi suunniteltiin machine-to-machine (M2M) –sovelluksiin. CoAP on avoin IETF –standardi, on luotu laajentamaan vaatimuksia, joita tarvitaan sulautetuissa laitteissa ja pienitehoisissa verkoissa. Tällä tarkoitetaan sitä, että CoAP:ssa voidaan käyttää samoja ajatusmalleja ja tekniikoita, kuin Webin perusprotokollan HTTP:n käytössä. CoAP –protokolla muistuttaakin rakenteeltaan hyvin läheisesti HTTP:tä. CoAP:sta löytyy tuki UPD:n (User Datagram Protocol), SMS:n (Short Message Service) ja TCP:n (Transmission Control Protocol) yhteiskäytön kanssa. Protokolla sisältää vahvan, sisäänrakennetun tietoturvan käyttäen DTLS:ää (Datagram Transport Layer Security). UDP –tuen takia, CoAP on täysin asynkroninen (engl. Asynchronous Subscription), eli ei-reaaliaikainen, jolloin tällä kyetään suorittamaan esimerkiksi monikanavaista lähetystä. (Shelby 2014)

CoAP:n arkkitehtuuri (Kuva 5) on hyvin suoraviivainen, jossa protokollaa voidaan käyttää peer-to-peer (vertaisverkko) laitteiden välissä, laitteen ja Web –palvelun välissä tai käyttää välityspalvelinta laitteen ja Web –palvelun välissä hyödyntäen HTTP:tä vuorovaikutuksessa. CoAP toimii käyttäen HTTP:n kanssa samoja metodeja, kuten GET, PUT, POST ja DELETE. Vaikka CoAP:in keskustelumalli on samantyyppinen kuin HTTP:llä, se ei ole yleinen korvike sille. HTTP:llä yksittäisen mittaus- tai ohjausarvon lähettäminen voi olla tehotonta, mikäli samalla halutaan lähettää tietoa laitteen hyväksymistä tietotyypeistä tai muista tiedoista. (Shelby 2014 & Syrjälahti 2015, 2.)



Kuva 5. CoAP –arkkitehtuuri.

CoAP:n kuljetuskerroksessa määritellään neljä erityyppistä viestiä: confirmable (vaatii ACK), non-confirmable (ei vaadi ACK), acknowledgement ja reset. CoAP voitaisiin ajatella kaksikerroksisena: viestikerros ja request/response kerros. Viestikerros huolehtii UDP:sta ja asynkronisista interaktioista. Request/response kerros käyttää koodeja Method ja Response. Tällä kerroksella tapahtuu REST (Representational State Transfer) –pohjainen kommunikointi. (Shelby 2014.)

HTTP:n suorituskyky CoAP:n kanssa			
Internet Protokolla yhdistelmä TCP/IP)		IP –pohjaiset älylaitteet Protokolla yhdistelmä	
Sovelluskerros	HTTP/FTP/SMTP/jne.	Sovelluskerros	CoAP
Kuljetuskerros	TCP/UDP	Kuljetuskerros	UDP
Verkkokerros	IPv4/IPv6	Verkkokerros	6LoWPAN
Siirtokerros	802.3, Ethernet/ 802.11, langaton LAN	Siirtokerros	IEEE 802.15.4e

Kuva 6. HTTP:n suorituskyky CoAP:n kanssa.

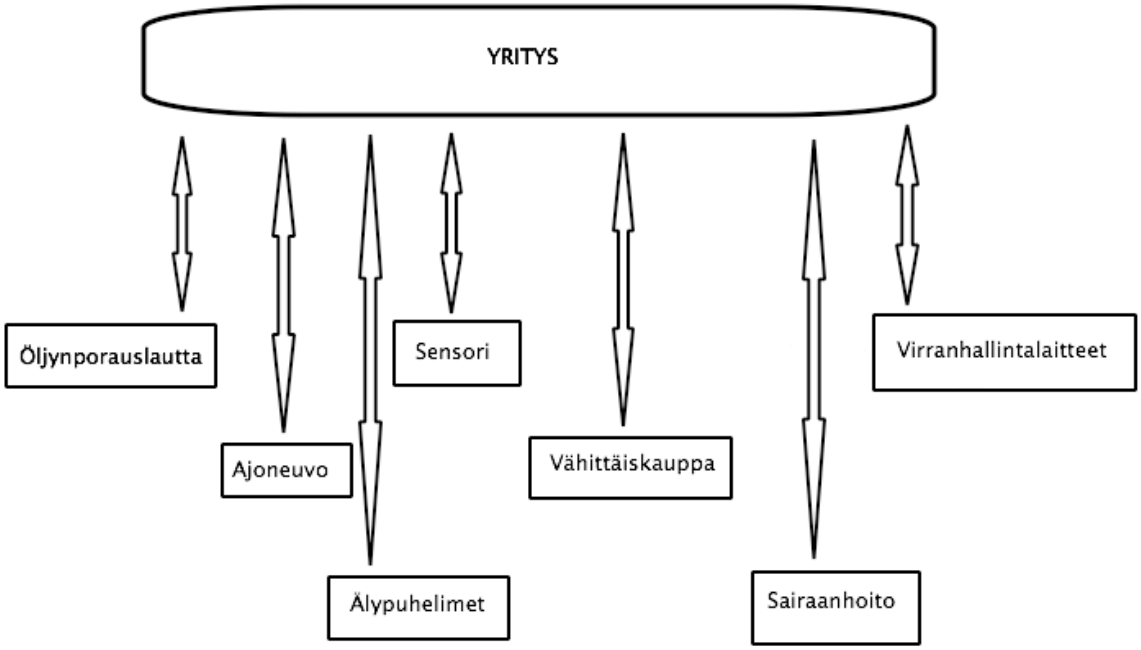
Colitti W. Vrije Yliopistosta vertasi HTTP: suorituskykyä CoAP:n kanssa ja teki kokeita IP –pohjaisten älylaitteiden protokollapinolla (Kuva 6). Kokeessa oli mukana CoAP –aktivoitu verkkoserveri. Kyseisessä kokeessa huomattiin CoAP:n vuorovaikutuksesta johtuen 42% pienempi virrankulutus. IoT –applikaatioon kuuluu jatkuva tiedonsiirto laitteesta toiseen liittyen tilaan, sisältöön tai sensoreiden mittauksiin. CoAP:sta löytyy toiminto, jolla asiakasohjelma (engl. the observer) voi rekisteröityä resurssiin (engl. the subject) modifioidulla GET -komennolla. Tällöin serveri luo ns. tarkkailutila –yhteyden ohjelman ja resurssin välille. Toiminnon avulla toimivuus on huomattavasti sujuvampaa, kuin esimerkiksi HTTP -pohjaisella yhteydellä. (Sutaria & Govindachari 2013, 3.)

Tutkimustuloksista on tullut ilmi, että CoAP –protokolla saadaan virraltaan tehokkaammaksi hyödyntäen sen kykyä pitää radiotaajuudet pois päältä mahdollisimman paljon. Käytännön kokeet paljastivat CoAP- ja muiden IoT –protokollien olevan 26 kertaa tehokkaampia, kun ne käyttävät kyseistä tekniikkaa. (Sutaria & Govindachari 2013, 3.)

3.3 MQTT

MQTT (Message Queue Telemetry Transport) on protokolla, joka keskittyy datan keräämiseen (Kuva 7) ja sen välittämiseen servereille. Nimensä mukaisesti sen tärkein tehtävä

on kaukomittaus ja etävalvonta (engl. remote monitoring). MQTT:n tavoitteena on kerätä dataa monista laitteesta ja välittää sitä IT –infrastruktuureihin. Kohteena ovat suuret verkot, joihin kuuluu pieniä laitteita, joita tarvitsee seurata tai ohjata pilvipalvelusta. (Schneider 2013, 3.)



Kuva 7. MQTT kuvaa hub-and-spoke –mallia.

MQTT ei yritä mahdollistaa laitteelta laitteelle tapahtuvaa tiedonsiirtoa tai levittää tätä usealle eri vastaanottajalle. MQTT:llä on hyvin selkeä yksi tehtävä ja on hyvin yksinkertainen protokolla, joka tarjoaa vain muutaman ohjausvaihtoehdon. Sen ei tarvitse myöskään olla kovinkaan nopea. Tässä tapauksessa termillä ”reaaliaika” tarkoitetaan sekunneissa tapahtuvaa toimintaa. (Schneider 2013, 4.)

Hub-and-spoke –arkkitehtuuri on luontaista MQTT:lle. Kaikki laitteet yhdistyvät datan keskittävään palvelimeen. Protokolla toimii TCP:n päällä, joka tuottaa yksinkertaista ja luotettavaa tietovirtaa, jotta yhtään dataa ei menisi hukkaan. Koska IT –infrastruktuuri käyttää tätä dataa, niin koko järjestelmä on suunniteltu välittää helposti dataa eri teknologiayrityksiin. MQTT mahdollistaa applikaatioita, kuten valvotaan isoja öljyputkia vuotojen tai vandalismin varalta. Kaikki käytössä olevat tuhannet sensorit tulee keskittää yhteen paikkaan analyysia varten. Kun järjestelmä havaitsee ongelman, se voi tehdä tarvittavat toimenpiteet sen korjaamiseksi. Muita MQTT:lla hyödynnettäviä kohteita ovat esimerkiksi virrankulutuksen monitorointi, valaistuksen hallinta ja jopa älykäs puutarhanhoito. Yhteistä näillä

on datan keruu useista eri lähteistä ja mahdollistaminen sen jakamisesta edelleen IT –infrastruktuureille. (Schneider 2014, 4.)

CoAP, toisin kuin MQTT, on käsitteellisesti eroteltu kahteen osa-kerrokseen: viestintäkerrokseen ja request-response –kerrokseen. Vastaan voi tulla tilanne, jossa pienitehoisen laitteen applikaatio käyttää MQTT –protokollaa sen täytyisi kommunikoida laitteen kanssa, joka ymmärtää vain CoAP –pohjaisia viestejä. Esimerkiksi älypuhelimen kautta käytettävä Facebook -applikaatio (Messenger -applikaatio) haluaa kommunikoida sekä usean ihmisen kanssa että Internetiä käyttävän laitteen kanssa. IoT:ssä kyse on kuitenkin ihmisten ja laitteiden saumattomasta vuorovaikutuksesta. (Sutaria & Govindachari 2013, 5.)

3.4 XMPP

XMPP (The Extensible Messaging and Presence Protocol) luotiin alun perin ihmisten väliseen pikaviestintään tekstiviestein. Nimensä mukaisesti protokollan käyttötarkoituksen ydin on ihmiskontakti (presence). XMPP käyttää XML tekstiformaattia alkuperäisenä tyyppinään, joten P2P –kommunikointi on sille luontaista. Samoin kuin MQTT, toimii myös XMPP TCP:n päällä. (Schneider 2014, 4.)

Esineiden Internetiin liittyen XMPP tarjoaa helpon tavan ”puhutella” laitteita. Kuten P2P –tapauksessa, tämä on erityisen kätevää jos data kulkee pitkälle, pääosin toisiinsa liittymättömien pisteiden läpi. Monet sovellukset käyttävät kiertokyselyä tai tarkastavat päivityksiä vain tarvittaessa, joten XMPP:tä ei ole suunniteltu varsinaisesti nopeaksi. (Schneider 2014, 5.)

Kotikäyttöön XMPP:n voidaan kuvitella tuovan hyvän vaihtoehdon esimerkiksi Web –server termostaatin, johon voidaan ottaa yhteys omalla älypuhelimella. XMPP:n vahvuudet löytyvät osoittamisesta (addressing), tietoturvasta ja skaalautuvuudesta. (Schneider 2014, 5.)

3.5 DDS

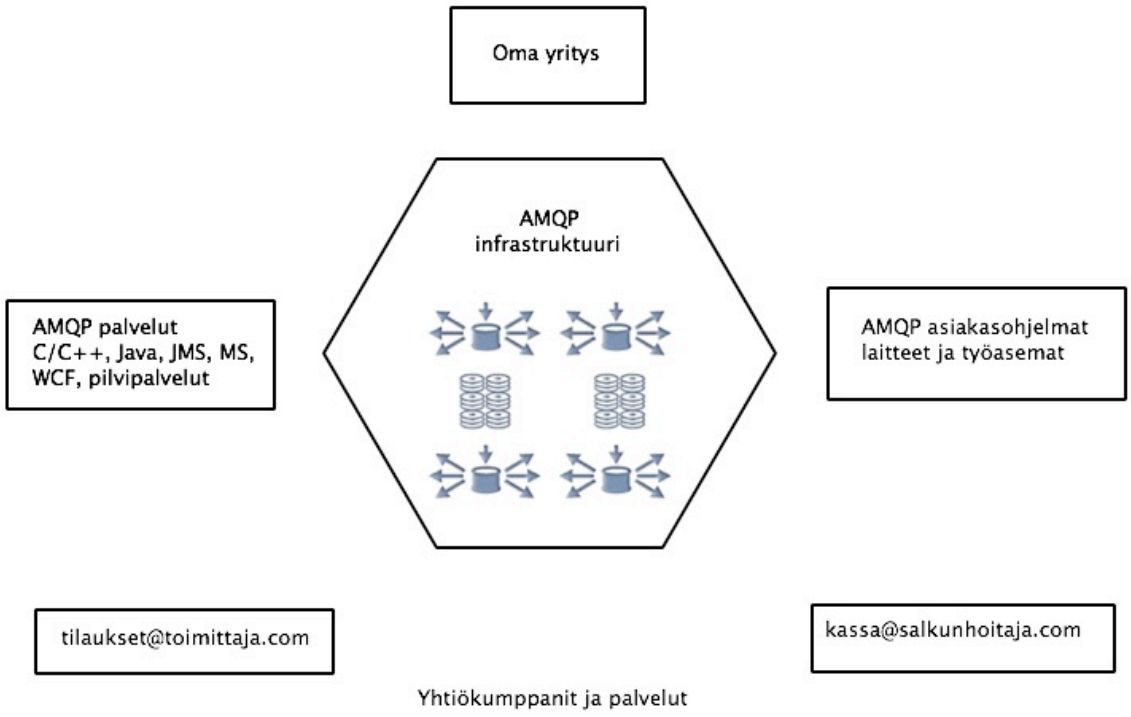
DDS (Data Distribution Service) on puolestaan kohdistettu laitteille, jotka käyttävät suoranaisesti laitedataa. Sen pääasiallinen tarkoitus on yhdistää laitteet keskenään. DDS pystyy tehokkaasti välittämään miljoonia viestejä sekunnissa useampaan vastaanottimeen samanaikaisesti. Laitteiden täytyy pystyä kommunikoimaan keskenään monin eri tavoin, joten TCP:n yksinkertainen point-to-point –virta on rajoittava tekijä. Sen sijaan DDS tarjoaa täsmällistä Quality-of-Service (QoS) -hallintaa, monilähetystä ja toimintavarmuutta.

DDS:n varmuuksiin kuuluvat vahvat suodattimet ja mahdollisuus määritellä mihin data menee, mikä voi tarkoittaa tuhansia eri kohteita samanaikaisesti. (Schneider 2014, 5.)

Tehokkaat integroidut laitejärjestelmät käyttävät DDS:ää. Se on ainoa tekniikka, joka tarjoaa joustavuutta, luotettavuutta ja tarvittavan nopeuden rakentaakseen monimutkaisia reaaliaikaisia sovelluksia. Sovelluksiin sisältyy sotilaallisia järjestelmiä, tuulivoimaloita, sairaaloita, lääketieteellisiä kuvauksia ja omaisuuden seurantajärjestelmiä. (Schneider 2014, 5.)

3.6 AMQP

AMQP (Advanced Message Queuing Protocol) perustuu jonoihin, jotka lähettävät tapahtumasanomia (haku ja tallennus) palvelimien välillä (Kuva 8). Viestikeskeisenä väliohjelmistona se pystyy käsittelemään tuhansia jonotusta vaativia tapahtumia. AMQP käyttää TCP:tä, joka antaa luotettavan yhteyden, jossa AMQP ei pääse kadottamaan viestejä. Päätelaitteiden tulee vahvistaa jokaisen viestin hyväksyminen. AMQP keskittyy siihen, että jokainen viesti saapuu perille huolimatta häiriöistä ja laitteiden uudelleenkäynnistyksistä. Tyypillisin AMQP:n käyttötarkoitus on liiketoiminnan viestien vaihdossa. IoT:n tapauksessa protokolla soveltuu parhaiten esimerkiksi palvelinpohjaisten analyysi –toimintojen suorittamiseen. (Schneider 2014, 6.)



Kuva 8. The Advanced Message Queuing Protocol (AMQP) on viestikeskeinen väliohjelmisto, joka on lähtöisin pankkialalta (Schneider 2014, 3).

4 Standardit ja IoT

Standardit toimivat koko esineiden Internetin käsitteen perustana. Internet itsessään toimii standardien pohjalta ja juuri standardit mahdollistavat laitteiden välisen kommunikoinnin. IoT:n kokonaisuutta voi olla vaikea hahmottaa, kun laitteet ja niiden eri osat ovat yhteyksissä ja vuorovaikutuksessa keskenään. Helpottaakseen ymmärrystä IoT:n voi jakaa neljään osaan: puettavat laitteet, älykodit ja kodinkoneet, ajoneuvot ja älykaupungit. (Bartleson 2014, 1.)

4.1 The Institute of Electrical and Electronics Engineers (IEEE)

Vuonna 1963 perustettu organisaatio The Institute of Electrical and Electronics Engineers (IEEE) on tunnettu mm. kehittämistään standardeista, ehkä tunnetuimpana IEEE 802.x työryhmä. 802.3 on IEEE:n standardi Ethernet –verkkoa varten, joka toimii lähes kaikkien lähiverkkojen (LAN) ja kaupunkiverkkojen (MAN) standardina. IEEE keskittyy erityisesti tiedonvälitykseen ja radiotekniikkaan. 802.11 on standardi langattomille WLAN - lähiverkolle, joka nykyään tunnetaan paremmin nimellä WiFi. ZigBee ja 6LoWPAN käyttävät 802.15.4 standardia, joka määrittelee langattoman PAN –verkon. (Reiter 2014, 5-6.)

Vuonna 2014 IEEE käynnisti uuden projektin P2413, jonka tavoitteena on luoda yhtenäinen arkkitehtuuri IoT –järjestelmille. Aiemmin IEEE on luonut useita kymmeniä standardeja, joita voidaan hyödyntää IoT –järjestelmissä, mutta ne ovat rakenteeltaan vertikaalisia ja koskevat vain erillisiä teknologiasaarekkeita. Vuonna 2016 valmistuvan P2413 –projektin tavoitteena on luoda puitteet ko. saarekkeiden väliselle yhteistoiminnalle, ristikkäiselle yhteiskäytölle ja toimintojen yhteensopivuudelle. (Lindstetd 2015, 2.)

4.2 The Internet Engineering Task Force (IETF)

The Internet Engineering Task Force on avoimen standardin organisaatio, joka vastaa Internet –protokollien standardoinnista ja toimii nykyisen Internetin perustana. IETF:n tekninen työ tapahtuu työryhmissä, joita ovat reititys, tietoliikenne ja turvallisuus. Työryhmät tuottavat Request for comments (RFC) –standardeja. RFC määrittelee tuhansia standardeja, kuten RFC 791, joka kuvailee IPv4 protokollan, RFC 793, joka kuvailee TCP protokollan ja RCF 2616, joka kuvailee http/1.1 protokollan. (IETF 2015 & Reiter 2014, 6.)

4.3 Kansainvälinen IoT -standardi

Standardiehdotus ISO/IEC NP 19654 annettiin vuoden 2014 alkupuolella ja sitä laaditaan kansainvälisessä työryhmässä ISO/IEC JTC 1 WG 5. Tämä työryhmä on erikoistunut juurikin Esineiden Internet -standardien laatimiseen. Alun perin standardin laatiminen aloitettiin siinä pelossa, että ilman ohjeistavaa standardia syntyisi saumattomammin yhteentoimivia erillisiä esineiden Internetejä. (Suomen Standardisoimisliitto 2014, 1.)

Standardi antaa ohjeita IoT -järjestelmien suunnitteluun ja kehittämiseen sekä edistää avointa ja julkista opastavaa arkkitehtuuria synnyttäen saumattomasti yhteentoimivia IoT –järjestelmiä. Lisäksi se pyrkii tekemään uusien komponenttien liittämisestä ja poistamisesta IoT –järjestelmiin mahdollisimman yksinkertaista. Hyötynä nähdään rakenteeltaan yhteensopivat järjestelmät sekä ajalliset ja rahalliset säästöt. Helpotuksena löytyy olemassa olevia IoT –arkkitehtuureja, joiden takia räätälöintiä ei tarvitse aloittaa alusta. Etuna tässä nähdään myös se, että riskit pienenevät kun hyödynnetään standardin hyviä käytäntöjä ja vältetään muiden tekemiä virheitä. (Suomen Standardisoimisliitto 2014, 1.)

4.4 Open Interconnect Consortium

Open Interconnect Consortium (OIC) on noin viidenkymmenen johtavan teknologiayhtiön liittouma, jonka tavoitteena on määritellä laitteiden yhteentoimiva IoT –maailma. Ensimmäisenä voimansa löivät yhteen Samsung, Intel ja Cisco, jotka julkistivat avoimen standardiprotokollan nimeltä IoTivity, joka mahdollistaa eri valmistajien laitteiden yhteensopivuuden. (Saroj, 2015, 1.) Merkittävänä huomiona voidaan pitää sitä, että IoTivity –projektia emännöi Linux Foundation, joka toimii suomalaisille tutun ohjelmoijan Linus Torvaldsin sponsorina. (Linux Foundation 2015, 1.) Open Interconnect Consortium –projektin tavoitteena olisi yhdistää seuraavat 25 biljoonaa laitetta eri teollisuusaloilla kuten terveys– ja energia-alalla. Ensimmäiset OIC:n ohjelmistot ovat kuitenkin kohdistettu koti– ja työympäristöihin. (Saroj 2015, 1.)

IoTivity:n käyttöä tuetaan mm. UDP/IP, CoAP ja MQTT –protokollilla. Runko on luotu C/C++:lla, mutta jotkut toiminnot tukevat myös Javaa. Toimintaperiaatteet IoTivity:n rungolle ovat luotu Esineiden Internet -komponenttien vuorovaikutukseen keskittyen. (Saroj 2015, 1.)

4.5 AllSeen Alliance

Vuoden 2014/15 Esineiden Internet -gaalassa loistavasti pärjännyt AllSeen Alliance sai mainintoja muun muassa paras avoin lähdekoodi –projektista sekä fiktiivisestä suunnitte-

lusta (IoT Awards 2015, 1). AllSeen Alliance on voittoa tavoittelematon liitto, joka haluaa kehittää Internet of Everything –konseptia kodeissa ja teollisuudessa. Liiton nimekkäimmät jäsenyhtiöt ovat mm. Microsoft, LG, Electrolux, Sony ja Qualcomm. AllSeen Alliancen mukaan yksikään tietty yhtiö ei pysty tuottamaan samaa yhteentoimivuutta mitä vaaditaan Internet of Everything –maailmassa. (AllSeen Alliance 2015, 1-2.)

Alunperin Qualcomm:in luoma AllJoy, jota AllSeen Alliance käyttää, on avoin ohjelmoitava ohjelmisto, jonka avulla yhtiöt voivat tuottaa yhteensopivia tuotteita, jotka sekä ovat yhteydessä että vuorovaikutuksessa keskenään. AllJoy on suunniteltu käsittelemään ongelmia, joita syntyy vertaisverkossa, kuten reititystä, turvallisuutta ja yhteentoimivuutta. AllJoyn tarkoitus on yksinkertaistaa laitteiden kommunikointia keskenään luvaten paremman käyttäjäkokemuksen. (AllSeen Alliance FAQs 2015, 2.)

4.6 Thread Group

Thread Group on organisaatio, jonka perustivat ARM Holdgins, Samsung ja Nest Labs (Google). Thread Group loivat Threadin eli verkon, joka yhdistää kotilaitteet tehokkaasti pienillä kustannuksilla ja virtaa säästävästi. Threadin protokolla on suunniteltu toimimaan valmiiksi markkinoilta löytyvältä sirulta, joka antaa oman IPv6 –osoitteen. Toimitusjohtaja Chris Borossin mukaan heidän tuotteitaan voitaisiin käyttää yhteistyössä AlllSeenin ja OIC:n kanssa. Thread Groupin laitteet kykenevät muodostamaan automaattisesti oman verkkonsa. (Lawson 2014, 2 & Thread Group 2015, 1.)

4.7 Z-Wave Alliance

Vuonna 2005 perustettu Z-Wave Alliance yhtiöiden liitto, joka keskittyy Z-Wave:n vakiinnuttamisen langattomien kotilaitteiden standardiksi. Yli 300 yhtiön liiton tärkeimpiä jäsenyhtiöitä ovat ADT, Evolve Guest Controls, FAKRO ja LG Uplus. Päätavoitteena näillä yrityksillä on tuottaa kotiin hallintalaitteita, joilla saadaan enemmän mukavuutta, energian säästämistä ja turvallisuutta. (Z-Wave Alliance 2015, 2.)

Z-wave on avoin standardi, joka on tällä hetkellä yksi suurimmista toimijoista langattomien kotituotteiden kehittämisessä kattaen yli 1200 sertifioitua yhteentoimivaa laitetta. Z-Waven laitteita ovat valot, ovien lukot ja termostaatit, ja nämä kommunikoivat keskenään langattomassa verkossa. Laitteita hallinnoidaan esimerkiksi älypuhelimella, tableteilla tai tietokoneilla. (Z-Wave Alliance 2015, 2.)

4.8 Industrial Internet Consortium

Indurstrial Internet Consortium on General Electric, Cisco System, IBM, Intel ja AT&T luoma yritys, jonka tavoitteena on saada teknologiamenetelmät toimimaan yhdessä sen sijaan, että asettaisivat omia standardeja. Hankkeeseen on liittynyt isoja yrityksiä kuten Microsoft, Samsung ja Huawei. Pyrkimyksenä on kehittää yhteistyötä toimialoilla, joissa IoT ja M2M –teknologiat ovat eristyneet toisistaan sisältäen standardien vaatimuksien määritystä ja luoden uusia testiympäristöjä applikaatioille. Lisäksi IIC haluaa kehittää ja määritellä referenssiarkkitehtuuria ja runkoja joita vaaditaan yhteentoimivuuteen. (Lawson 2014, 2 & Industrial Internet Consortium 2015, 1.)

4.9 Avoimen standardin IoT

Esineiden Internet tuo mukanaan suuren määrän yrityksiä taistelemaan markkinaosuuksista. Sarojin (2015, 1) mukaan kuukausia kestänyt standardisota yhtiöiden välillä voisi olla lähellä loppuaan. Jo valmiiksi laaja ja monipuolinen teollisuus tuottaa varmasti sekaannusta, kun yhtiöt pyrkivät tuomaan omia ratkaisujaan IoT –maailmaan. Tarkoitus on yhdistää laitteet keskenään, mutta myös kehittää näiden laitteiden ohjaamia applikaatioita. Ennen pitkään eri toimittajien olisi päästävä samalle linjalle ainakin jossain määrin. Lawson kuitenkin näkee uhkakuvia siitä, miten tuotantoa ei saada linjausten poikkeavuuksista johtuen tehostettua niin, että hinnat saataisiin alas. Kustannuskysymys tulee olemaan kuitenkin se tärkein tekijä tässäkin teollisuudessa. (Lawson 2014, 1.)

Saroj näkee selkeän jaottelun tulevaisuudessa, jossa kaksi standardia taistelevat jalansijasta esineiden Internet -maailmassa. Etulyöntiasemassa olisi Sarojin mukaan AllSeen Alliance, jolta löytyy satoja jäseniä OICn kymmeniä vastaan. Molemmilla yhtiöillä oletetaan oleva sama päämäärä eli toteuttaa järjestelmäriippumaton väliohjelmisto yhdistääkseen erilaiset ohjelmistoapplikaatiot langattoman protokollan kautta. Eroavaisuutena näillä organisaatioilla olisi halu myydä halvalla patentteja standardeille, jossa OIC olisi selkeästi innokkaampana mukana kuin AllSeen Alliance. (Saroj 2015, 1.)

5 Langattomat tekniikat IoT:ssä

Nopeasti kasvavassa esineiden Internetissä sovellukset, esineet, laitteet ja sensorit ottavat yhteyden toisiinsa verkon kautta. Koska kyse on niin laajasta verkkoympäristöstä ja tarpeista, niin tarvitsemme monta eri langatonta tiedonsiirtotekniikkaa. Markkinoilla on jo esitetty monta eri standardivaihtoehtoa, jotka käyttävät eri protokollia. Tästä syystä on haastavaa saada oikea tiedonsiirtotekniikka käytettäville IoT -laitteille. Jokaisella tekniikalla on omat etunsa, mutta mikään ratkaisu ei ole täydellinen. Tärkeintä onkin löytää paras vaihtoehto omiin ratkaisuihin. (Reiter 2014, 1.)

5.1 WiFi Alliance

Vuonna 2015 tuli kuluneeksi 16 vuotta WiFi Alliancen perustamisesta. 1999 luotu WECA (Wireless Ethernet Compatibility Alliance) sai siitä seuraavana vuonna uuden käyttönimen WiFi Alliance WiFi –termin myötä. Organisaatioon kuuluu yli 600 jäsenyritystä, jotka ovat sertifioineet yli 25,000 tuotetta. (WiFi Alliance 2015, 1.)

5.1.1 WiFi ja IoT

WiFi on luotu alusta alkaen toimimaan Internet -yhteytenä. WiFin käyttö yleistyi rajusti älypuhelimien ja tablettien myötä ja nykyään se on käytössä jo lähes joka kodissa, työpaikalla, kouluissa, lentokentillä ja kahviloissa. WiFi käyttää IEEE 802.11 –standardia, joka korvasi Ethernet –standardin IEEE 802.3. (Reiter 2014, 7.)

Seuraava askel WiFin käyttöön on yhdistää IoT –ratkaisuissa käytettävät sensorit ja laitteet. WiFin käyttämä ohjelmisto on suhteellisen iso ja suurilla mikroprosessoreilla varustetut laitteet, kuten kannettavat tietokoneet ja älypuhelimet toimivat ongelmitta. Nykyään on myös mahdollista lisätä WiFi –ominaisuus myös laitteisiin, joissa on pienempi prosessori, kuten termostaatit ja kodinkoneet. Uudet pienemmät mikrosirut, joihin on upotettu WiFi ja TCP/IP -ohjelmistot mahdollistavat nykyään langattoman verkon toimivuuden. (Reiter 2014, 7.)

WiFi kuluttaa suhteellisen paljon virtaa luodakseen nopean ja kattavan sisäyhteyden. Jotkut pattereilla toimivat IoT -laitteet kuluttavat liikaa virtaa WiFi -yhteydellä. Mikrosiruihin on lisätty virrankulutusta säästävää tekniikkaa kuten lepotila ja nopeat käynnistys ja lopetustoiminnot. Näiden virranhallintaratkaisuiden takia suurin osa IoT –tuotteista voi toimia yli vuoden käyttämällä kahta AA –patteria. (Reiter 2014, 7.)

5.1.2 WiGig

WiFi Alliance tuo uuden WiGig –nimellä tunnetun IEEE 802.11ad –standardin, joka on tarkoitettu mm. älykoteihin, IoT- ja tietoliikennekäyttöön. Samsungin mukaan uudet 60 GHz:n tekniikalla varustetut WiFi –laitteet ovat yli viisi kertaa nykyistä 802.11ac –standardia nopeampia. Laitteiden teoreettinen tiedonsiirtonopeus on 575 Mt/s verrattuna aiempaan 108 Mt/s. Samsungin mukaan laitteiden lisääminen verkkoon ei hidasta tiedonsiirtonopeuksia yhtä paljon kuin nykyisillä tekniikoilla. Esimerkkinä Samsung esittää 1GB elokuvan siirron kestävän alle kolme sekuntia. (Jäntti 2014, 1 & Gigaom 2014, 1 - 2.)

Haittapuolena Samsung toteaa olevan 60 GHz taajuuden käyttö, joka vaatii signaalin läpäisykykyyn suoran linjan. Kyseisen signaalin häiriöinä toimivat seinät, vesi ja jopa happi. Parantaakseen ongelmaa Samsung on kehittänyt muun muassa laajan säteen antennin. (Jäntti 2014 & Gigaom 2014, 1-2.)

5.2 Bluetooth

Ericsson keksi Bluetooth teknologian 1994 langattomaksi yhteydeksi puhelimien ja tietokoneiden välille. Syy miksi Bluetooth:in käytöstä tuli niin suosittua aluksi olivat hands-free puhelut langattomilla kuulokkeilla. Myöhemmin mukaan tuli käyttöön esimerkiksi musiikin suoratoisto. (Bluetooth.com 2015, 1.)

5.2.1 Bluetooth Special Interest Group

Bluetooth Special Interest Group (SIG) perustettiin 15 vuotta sitten ja se valvoo Bluetooth -spesifikaatioiden kehitystä sekä Bluetooth -brändin mainostamista ja suojaamista. Bluetooth SIG:llä on yli 25,000 jäsenyritystä yhteistyössä langattoman tekniikan parissa. (Bluetooth.com 2015, 1.)

5.2.2 Bluetooth ja IoT

Bluetooth kuuluu PAN verkkoon ja kykenee siirtämään dataa 2Mb/s. Bluetoothin pystyy yhdistämään useampaan laitteeseen kerralla, mutta suositeltu määrä on 10 ja 20 laitteen välillä. Miten Bluetooth sitten liittyy esineiden Internetiin? Se yhdistää langattomia lisälaitteita älypuhelimiin ja tabletteihin, jotka toimivat porttina Internetiin. Hyvinä esimerkkeinä toimivat muun muassa sydänmonitori, joka lähettää dataa pilviserveriin, tai puhelimen välityksellä toimiva ovenlukitusjärjestelmä, joka on suorassa yhteydessä turvallisuusalan yhtiöön. Tuotevalmistajilla on hyvä lähtökohta luoda IoT –ratkaisujaan, koska nyt on jo olemassa suuri määrä Bluetooth –ominaisuudella varustettuja laitteita. (Reiter 2014, 8 & Bluetooth.com 2015, 1.)

Laajentaakseen ja kasvattaakseen potentiaaliaan IoT –markkinoilla, Bluetooth SIG aloittaa työstämään Mesh –verkon yhdistämistä tekniikkaansa. Bluetooth soveltuu hyvin IoT –järjestelmiin pienen virrankulutuksen ja älylaitteiden yhteensopivuuden takia. Bluetooth:in toimintasäde rajoittuu kuitenkin vain muutamaan kymmeneen metriin ja sen täytyy organisoitua ”hub-and-spoke” –malliin, jossa integraatiojärjestelmä toimii keskitettynä pisteenä ja dataintegraatio tapahtuu. Tällä tavoin useiden tietovirtojen hallinta ja valvonta mahdollistuu keskitetystä pisteestä. ZigBee ja 6LoWPAN kykenevät jo luomaa laajempia verkkoyhteyksiä linkittäen laitteita yhteen. (Lawson 2015, 1.)

Mesh –verkossa esineet kuten termostaatit ja valot kommunikoivat keskenään ottamatta yhteyttä lähellä olevaan tietokoneeseen, jolloin verkot ovat helpompia ja halvempia rakentaa. Tästä syystä Thread Group siirtyi käyttämään 6LoWPAN:ia siitä huolimatta, että se ei ole samalla tavalla saatavilla kuin Bluetooth. Uudet ominaisuudet ovat tarkoitettuja lähinnä Bluetooth Smart –tuotteille. Eniten hyötyä juuri mesh –verkon käytöstä saisivat laitteet, kuten sensorit ja hehkulamput. Bluetooth SIG:n markkinointijohtaja Kroeterin mukaan todennäköisesti jo olemassa olevat Bluetooth Smart –laitteet päivitettäisiin käyttämään mesh –verkkoa. (Lawson 2015, 1.)

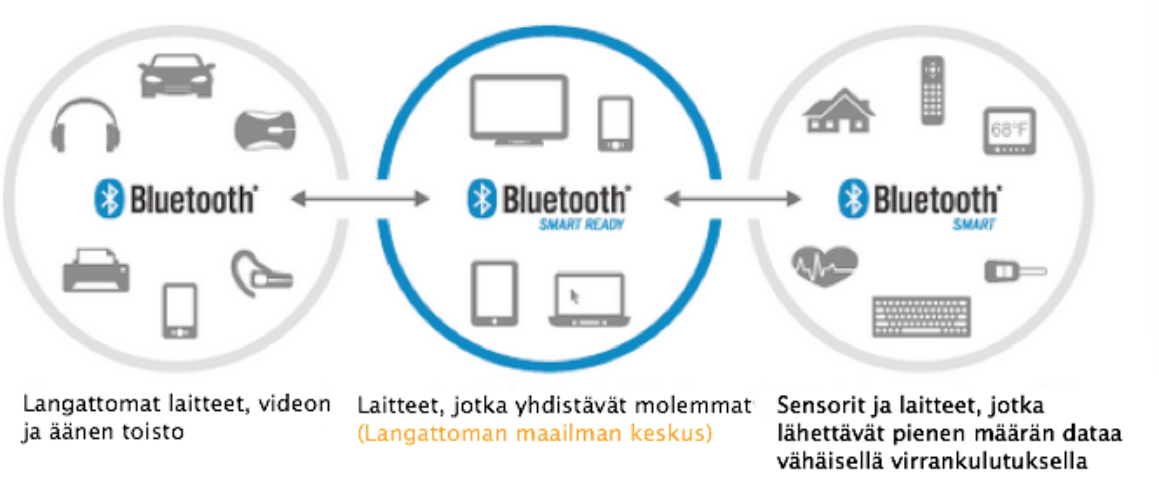
Bluetooth SIG on luonut työryhmän Bluetooth Smart Mesh –verkolle, jonka odotetaan tuovan kyseistä tekniikkaa laitteisiin vuoden 2016 kuluessa (Lawson 2015, 1).

5.2.3 Bluetooth Smart

Bluetooth Smart (Low energy) laitteet ovat suunniteltu keräämään kohdistettua informaatiota, kuten ovatko kodin ikkunat lukitut tai paljonko ihminen painaa. Informaatio lähtee suoraan Bluetooth Smart:in kanssa yhteensopivaan laitteeseen, kuten älypuhelimeen tai tablettiin. Bluetooth Smart vie pidemmälle langatonta tekniikkaa pienellä kolikkomaisella koollaan ja hyvin alhaisella virrankulutuksella. Toisin kuin klassisella Bluetooth:lla, niin Bluetooth Smart:lla saadaan toimintasäde paljon laajemmalle (yli 60 metriä). Valmistaja lupaa alhaisen virrankulutuksen lisäksi myös hyvän yhteensopivuuden laitteiden kanssa ja alhaiset kulut. (Bluetooth.com 2015, 1-2.)

Kyseistä Bluetooth Smart –tekniikkaa hyödyntävä Polar on tuonut markkinoille muun muassa juoksu- ja sykesensorin. Sensorit kiinnitetään joko jalkaan tai ranteeseen ja nämä lähettävät dataa reaaliajassa harjoitustietokoneelle tai älypuhelimeen. (Polar 2015, 1 & Bluetooth.com 2015, 1.)

Seuraavasta kuvasta (Kuva 9) ilmenee, miten Bluetooth smart:in kanssa yhteensopivat laitteet saadaan yhdistettyä muihin Bluetooth –laitteisiin (Bluetooth.com 2015, 1).



Kuva 9. Bluetooth -laitteiden yhteensopivuus (Bluetooth 2015, 1).

5.3 Wifi ja Bluetooth yhdessä (Atmel WINC1500)

Esineiden Internet –laitteisiin on nyt suunniteltu moduuli, joka tukee käytännössä kaikkia WiFi –salauksia (WEP,WPA ja WPA2) ja IEEE 802.11 –standardia. Atmelin WINC1500 –moduuli on rinnakkain WiFi- ja Bluetooth –radiosignaaleja käsittelevä siru, joka on hyvin tiukkaan pakattu. Kooltaan siru on vain 21,5 x 14,5 x 3,4 –millinen. Hyvin pienellä virrankulutuksella varustettu moduuli tulee toimeen 4 mikroampeerilla. (Etn 2015, 1 & Mouser 2015, 1-2.)

5.4 6LoWPAN

6LoWPAN on ensimmäinen langaton standardi, joka on kehitetty nimenomaan IoT:tä varten. 6LoWPAN on kirjainlyhenne, jossa yhdistyy IPv6 –protokolla ja LoWPAN (Low-power Wireless Personal Area Networks). Tämä kirjainlyhenne voi olla hieman hämmennystä herättävää koska 6LoWPAN käytetään normaalisti LAN:ssa (Local Area Network). The Internet Engineering Task Force:n (IETF) 6LoWPAN –työryhmän luoma standardi mahdollistaa pienimpien laitteiden, joilla on rajattu prosessointikyky, välittää langattomasti informaatiota käyttäen Internet -protokollaa. 6LoWPAN pohjautuu Internetin OSI-mallin siirtoyhteyskerroksen määrittelyyn RFC 6282. Kommunikointi tapahtuu laitteiden välillä, jotka käyttävät 802.15.4 –standardia. Vaikka 6LoWPAN –laitteet olisivat eri verkoissa ne pystyvät kommunikoimaan keskenään. Lisäksi 6LoWPAN –laite pystyy kommunikoimaan minkä tahansa IP –pohjaisen serverin tai laitteen, mukaan lukien WiFi- tai Ethernet –laitteiden kanssa. (Reiter 2014, 8-9.)

6LoWPAN tukee ainoastaan IPv6 –protokollaa johtuen osoitteen pituudesta ja osoiteavaruuden laajuudesta. Toinen syy tähän on sisäänrakennettu tuki verkon automaattiselle asennukselle. Saadakseen yhteyden Internetiin 6LoWPAN vaatii Ethernet- tai WiFi –portin. Valtaosa käyttöönotetusta Internetistä käyttää yhtä IPv4 –protokollaa, joten 6LoWPAN –porttiin on asennettu ”IPv6-to-IPv4” konvertointi. (Reiter 2014, 9.)

Uusimpana kilpailijana muun muassa ZigBee:lle 6LoWPAN käyttää sekä 2.4-GHz että 868-MHz/915-MHz taajuuksia. 6LoWPAN:in etuihin lukeutuu 802.15.4 –standardin käyttö, suuri verkon koko, luotettava yhteys ja pieni virrankulutus. Näiden johdosta 6LoWPAN on hyvässä asemassa verkkoyhteydessä olevien sensoreiden ja muiden paristoilla toimivien applikaatioiden osalta. (Reiter 2014, 9.)

5.5 ZigBee

ZigBee on saanut nimensä mehiläisten mukaan. Mehiläisten yhdyskunnassa selviytyminen ja tulevaisuus ovat riippuvaisia niiden jatkuvasta keskinäisestä kommunikoinnista. Mehiläisten käyttämiä tekniikoita, jossa informoidaan uusista ruokapaikoista yhdyskunnan jäsenille kutsutaan nimellä ZigBee. Käyttäen tätä tehokasta, mutta hiljaista kommunikaatiota, mehiläiset voivat viestiä keskenään ruokapaikan etäisyydestä, olinpaikasta ja suunnasta. (UKessays 2015, 1.)

5.5.1 ZigBee Alliance

ZigBee Alliance on organisaatio, joka pyörittää sertifiointi –ohjelmaa laitteiden yhteentoimivuuden takaamiseksi. Tähän Allianssiin kuuluu suuria yrityksiä kuten Samsung, Intel, HP ja Philips. Ensimmäisen standardin määritys valmistui vuonna 2004. ZigBee Alliance on avoin jäsenilleen, jonka jäsenvuosimaksut alkavat 4000 dollarista. (ZigBee Alliance 2015, 1.)

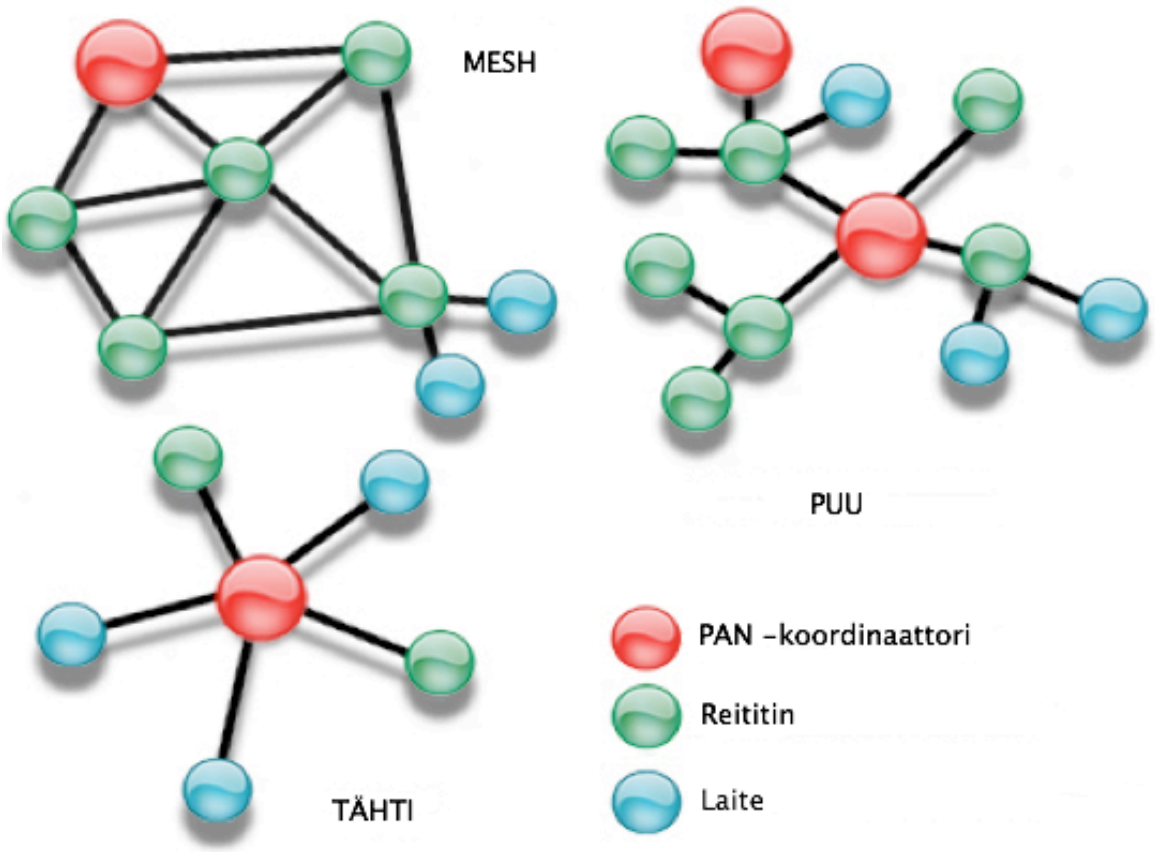
5.5.2 ZigBee ja IoT

ZigBee Alliancen ylläpitämä ZigBee:n tarkoituksena on määritellä OSI-mallin verkkoyhteys- sekä kuljetuskerrokset. Samoin kuin 6LoWPAN, niin ZigBee pohjautuu myös 802.15.4 –standardin käyttöön. ZigBee on lyhyen kantaman tietoliikenneverkko, joka määrittelee pienitehoisen WPAN:n. Pääosin se toimii 2.4-GHz taajuudella, mutta tuki löytyy myös 868-MHz ja 915-MHz taajuuksille. ZigBee on toistaiseksi suosituin standardi markkinoilla edullisuuden ja vähän virtaa kuluttavien ominaisuuksien vuoksi. Yksi isoimmista eroista ZigBee:llä 6LoWPAN:iin on sen rajoitettu kyky kommunikoida muiden protokollien kanssa,

vaikka ZigBee:n IP pohjautuu IEEE 802.15.4 –standardin käyttöön. ZigBee:hin on rakennettu ominaisuus, jolla se pystyy olemaan pitkiä aikavälejä lepotilassa ja näin toimimaan kuukausista jopa vuosiin paristoilla. (ZigBee Alliance 2015, 1 & Reiter 2014, 9.)

ZigBee -verkossa on kolme erilaista laitetta: ZigBee Coordinator (ZC), ZigBee Router (ZR) ja ZigBee End Device (ZED). ZC on vastuussa verkon muodostamisesta sekä verkon tietojen säilyttämisestä. Näitä laitteita on yksi jokaista ZigBee -verkkoa kohden. ZR –laitteen tehtävänä on huolehtia datan reitittämisestä muille laitteille. ZED –laite on yksinkertainen, joka vaatii vähemmän muistia kuin ZC tai ZR. (ZigBee Alliance 2015, 1.)

ZigBee -tekniikassa on käytössä kolme verkkotopologiaa: tähti, puu ja mesh. Yksinkertaisin näistä on tähtitopologia, jonka verkossa tapahtuva liikenne on eniten rajoitettua. Päätelaitteet kykenevät kommunikoimaan vain koordinaattorin kanssa, joten kaikki verkkoliikenne kulkee koordinaattorin kautta. Puutopologiassa verkko koostuu koordinaattorista, useista reitittimistä ja päätelaitteista. Päätelaitteet kommunikoivat reitittimen välityksellä, jolloin koordinaattorin kautta kulkeva verkkoliikenne vähenee. Toisin kuin tähtitopologiassa, niin verkko ei ruuhkaudu samalla tavalla puutopologiassa. ZigBee:n tärkeimpänä osana on Mesh –topologia (Kuva 10), jota kutsutaan myös peer-to-peer –verkoksi. Tiedonsiirron turvallisuutta lisäten verkossa tapahtuva liikenne on mahdollista toteuttaa useita eri reittejä pitkin. (Elahi & Gschwender 2009, 1-2.)



Kuva 10. Kolme verkkotopologiaa määriteltynä IEEE 802.15.4 –standardissa (ICPDAS-USA 2015, 1).

Erityisesti IoT –sovelluksiin kehitetty ZigBee 3.0 yhdistää aiemmat ZigBee –versiot saman määrityksen alle. Tämä pohjautuu IEEE 802.15.4 standardiin, joka toimii 2.4 GHz -taajuudella. ZigBee Alliance lupailee uusimman version luovan saumattoman yhteentoimivuuden pitkän kantaman älylaitteiden verkossa sekä antavan kuluttajille ja yritykselle pääsyn tuotteisiin ja laitteisiin, jotka toimivat mutkattomasti yhteen. Vuoden 2015 lopulla valmistuva versio 3.0 on tällä hetkellä testivaiheessa ZigBee –yhteisön jäsenyhtiöillä. (ZigBee Alliance 2015, 1 & Lindstedt 2015, 3.)

6 Referenssimalli IoT:lle

6.1 IEEE P2413

IEEE:n IoT –arkkitehtuurityöryhmä luo P2413 -standardin referenssimallin (engl. Reference model) IoT:lle. Useimmat nykyiset standardoinnit rajoittuvat johonkin tiettyyn toimialaan. Tässä standardissa määritelty arkkitehtoninen runko edistää toimialueiden vuorovaikutusta, tukijärjestelmien yhteentoimivuutta ja toiminnallista yhteensopivuutta ja tulee näin edistämään IoT –markkinoiden kasvua. Yhtenäinen lähestymistapa IoT –järjestelmien kehittämisellä vähentää alojen hajanaisuutta. Standardi määrittelee arkkitehtonisen rungon IoT:lle, johon kuuluu kuvaukset monille IoT –toimialueille, määritelmät toimialueiden abstraktioille ja yhtäläisyyksien tunnistamisen eri IoT –toimialueiden välillä. Arkkitehtoninen runko tarjoaa referenssimallin, joka määrittelee eri toimialojen suhteita, kuten kuljetus ja terveydenhuolto. Lisäksi standardi tarjoaa referenssiarkkitehtuurin, joka perustuu referenssimalliin. Tavoitteena on lisätä järjestelmäarkkitehtuurin näkyvyyttä, jotta saadaan tukea suorituskyvyn mittaamiselle, turvallisuudelle ja turva-arvioinneille. (IEEE 2015, 1.)

IEEE P2413 kuuluu paljon jäsenyhtiöitä, kuten Cisco Systems, Huawei Technologies, Qualcomm Inc. ja Siemens AG. Vauhdittaakseen kehitysprosessia P2413 on käynnistänyt useita alatyöryhmiä, kuten soveltamisala ja sovellettavuus, verkostoituminen ja referenssimalli. Työn valmistumisen aikajana on asetettu vuodelle 2016. (IEEE 2015, 1.)

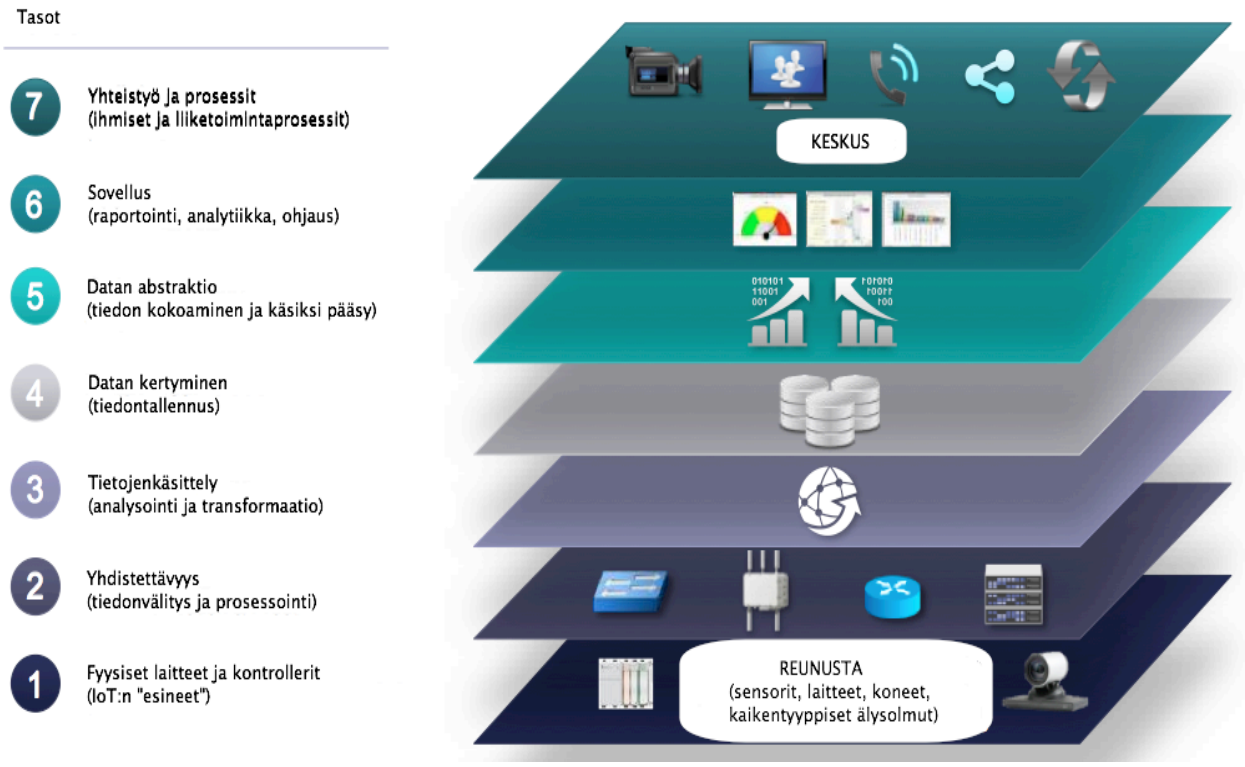
6.2 IoTWF

Internet of Things World Forum (IoTWF) –johtajat julkaisivat Chicagossa vuoden 2014 lokakuussa uuden referenssimallin IoT:lle. Teollisuusjohtajat julkaisivat keskeisiä aloitteita, joilla saadaan koko ala siirrettyä laaja-alaisempaa käyttöönottoa varten. Tämä vaatii uutta teknologiaa, teollista ekosysteemiä, lahjakkuutta ja koulutusta. IoTWF –tapahtuma esittelee tosielämän käyttöönotto –skenaarioita, jotka ovat jo antaneet arvon sekä julkisella että yksityisellä sektorilla. IoT –ratkaisuiden etuihin, kun kyseessä on uusien toimintamallien luonti, voisi luetella esimerkiksi ajotehokkuuden ja paremman elämänlaadun. (Cisco / IoTWF 2014, 1.)

IoTWF, jossa Cisco toimii isäntänä, tuo yhteen monia alallaan arvostettuja ajattelijoita, ammattilaisia ja keksijöitä. Edistääkseen IoT –markkinoita, johtajat Intel:stä, Rockwell Automation:sta ja Schneider-Electric:stä kokoontuvat konferenssiin yhdessä suurten yhtiöiden kanssa, kuten Shell ja Rio Tinto. Vuoden 2014 IoTWF avaintapahtuma Barcelonassa

houkutteli kolminkertaisen määrän asiakkaita ja sponsoreita aiempaan vuoteen verrattuna. (Cisco / IoTWF 2014, 1.)

IoTWF julkaisema referenssimalli (Kuva 11) IoT:lle toimii yleisenä kehyksenä kehittääkseen IoT –alaa. Tämän referenssimallin tarkoitus on kehittää liiketoiminnan arvoa nopeuttamalla kopioituja käyttöönottomalleja ja edistämällä sekä teollisia innovaatioita että yhteistyötä luomalla avoimen ja yhteisen luokittelun (engl. taxonomy). Mallin pyrkimyksenä on tarjota yhteinen terminologia ja tuoda selkeyttä siihen miten informaatio virtaa ja miten sitä prosessoidaan. Tavoitteena on päästä yhtenäisempään IoT –teollisuuteen. Vastauksia pitäisi myös saada käytännön ehdotuksiin siitä, miten skaalautuvuuden ja yhteentoimivuuden haasteisiin vastataan, kun suuret yritykset pyrkivät julkaisemaan omia IoT –ratkaisuja. Aloitteen tavoitteena on lisäksi määritellä ”avoimen järjestelmän” IoT, jossa useammat yhtiöt voivat olla osallisena ja ottaa ensiaskeleet kohti IoT –tuotteiden yhteentoimivuutta tavarantoimittajien kesken. (Cisco / IoTWF 2014, 1.)



Kuva 11. Ciscon IoT -referenssimalli (Cisco / IoTWF 2014)

7 Virranhallinta IoT -laitteissa

Esineiden Internetin on tarkoitus yhdistää koko ympäristömme maailmanlaajuiseen tietoverkkoon, mutta pyrkimysten hidastuksina ovat mm. ratkaisemattomat ongelmat esineiden teholähteissä. Monien IoT –laitteiden energiabudjetti on hyvin rajoittunut, koska ne toimivat pariston, akun tai toimintaympäristöstä kerätyn energian varassa, ja tämä johtaa pienitehoisten prosessoreiden ja kohtuullisen hitaiden yhteystapojen kautta kevyiden ratkaisujen käyttöön tiedonsiirrossa. IoT –laitteissa pyörii usein suoraan raudan päälle kirjoitettu ohjelmisto tai kevyt reaaliaikakäyttöjärjestelmä. (Syrjälahti 2015, 1-2.)

Useimmat IoT –laitteet tulevat olemaan pääosin paristokäyttöisiä, joiden pitää toimia useita vuosia ilman erillistä ylläpitoa tai paristonvaihtoa. Jotta laite saadaan toimimaan pitkiä aikoja yhdellä latauksella, sen on kulutettava mahdollisimman vähän tehoa. Jotkut IoT –laitteet saavat virtansa ulkoisesta lähteestä prosessilla, jota kutsutaan energiankeruuksi. Molemmissa tapauksissa energiatehokkuus on ehdottoman tärkeää, jotta IoT:n potentiaali saadaan kokonaan esiin. (Lattice 2015, 3.)

Energiatehokkuus, koko ja kustannus ovat IoT:n keskeisimpiä haasteita. Tulevina vuosina IoT tuo käyttäjilleen hyvin erilaisen kokemuksen, jossa tarjotaan parempaa liitettävyyttä, yksinkertaisuutta, käyttömukavuutta, jatkuvaa verkossa oloa tai ainakin mielikuvan siitä. Ajatuksena laitteen päällä olo on huomattavasti houkuttelevampi kuin sen toistuva aktivointi ja sulkeminen nappia painamalla. Tämä aina-päällä –vaatimus ajaa tarvetta parantaa energiatehokkuutta. IoT –laitteet eivät yksinkertaisesti voi olla jatkuvasti päällä ja yhteydessä verkkoon, elleivät ne voi operoida erittäin pienellä teholla saaden virran paristoista tai ulkoisesta lähteestä. (Lattice 2015, 4.)

Älykäs aistiminen ja big data –analyytikot tulevat olemaan isossa roolissa, sillä ne mahdollistavat älykkäämmän datan keruun, niin että trendejä tai merkittäviä tapahtumia voidaan nopeasti tunnistaa ja tarpeen mukaan toimia niiden pohjalta. Energiatehokkuus on tässäkin kohtaa keskeistä, sillä datan keruu vaatii tehoa, niin kuin muisti johon data tallennetaan. (Lattice 2015, 4-5.)

Riittävän energiatehokkuus IoT –laitteille, jotta ne toimisivat vuosia, tulee olemaan iso haaste. Vaatimuksena ovat pienitehoisten komponenttien käyttö ja hyötysuhteeltaan parempien tehojärjestelmien kehitys. Lisäksi edellytyksenä on muutoksia sekä arkkitehtuurin että komponenttien tasolla. Tähän päivään mennessä jokaisessa IoT –laitteen suunnittelun vaiheessa on keskitytty mahdollisimman suureen energiatehokkuuteen. Esimerkiksi

älypuhelimille tämä tarkoittaisi kertaluokkaa parempaa energiatehokkuutta, mikä ei tule tapahtumaan hetkessä. Päinvastoin kehitys tapahtuu askelittain ja vaatii useiden laitesukupolvien kehitystyön. (Lattice 2015, 5.)

Lattice Semiconductor, joka toimii energiatehokkaiden ohjelmoitavien komponenttien johtajana, työskentelee alentaakseen tehonkulutusta IoT –liitäntälaitteissa. Tällä hetkellä Yritys keskittyy löytämään uusia tapoja parantaa energiatehokkuutta esimerkiksi prosessitekniikan innovaatioiden ja transistorien tasolla. Lattice pyrkii tuomaan lisää vapautta järjestelmäsuunnittelijoille ohjelmoitavan nopeuden ja teho –ominaisuuksien muodossa. Tämän lisäksi Latticen tavoitteena on kehittää arkkitehtuuria mahdollistaen älykkään tehonhallinnan eri tiloissa, joissa laitteet todella ovat. (Lattice 2015, 5.)

Washingtonin yliopiston tutkijat suunnittelevat uusia tapoja, joilla voidaan vähentää akkujen vaihtamista. Kehitteillä on uusi WLAN –tekniikka, joilla esineet keräisivät viestintään tarvittavan tehon ympäristönsä radiosignaaleista. Kunnianhimoinen tavoite tämän tekniikan avulla olisi yhdistää verkkoon miljardeja laitteita ilman paristonvaihdon tarvetta. WiFi backscatter –nimellä kulkeva tekniikka muuttaa radio-, tv- ja WiFi –signaaleja sähköksi. Tekniikka toimii nykyisellään pienen, elektroniikkaa ja antennin sisältävän ”lätkän” avulla, jonka kommunikointi WLAN –reitittimen kanssa toimii äärimmäisen pienellä tehonkulutuksella. Washingtonin yliopiston tutkijoiden mukaan WLAN -tukiasemien päivittäminen tukemaan uutta teknologiaa madaltaisi kynnystä sen käyttöönottoon. Toistaiseksi tutkijat ovat onnistuneet WLAN –laitteiden kanssa viestimisen 1 kbps nopeudelle kahden metrin etäisyydellä, mutta tarkoitus olisi parantaa sitä noin 20 metriin. (Laitila 2015, 1.)

8 IoT:n tietoturva

Haasteita tulee varmasti riittämään turvallisuuden ylläpitämisessä samaan aikaa, kun Esineiden Internet pyrkii tulemaan jokapäiväiseksi osaa meidän elämää ja yhteiskuntaa. Niin kuin kaikki uusi ja erilainen myös IoT tulee saamaan myös vihollisia horjuttamaan systeemiä tavalla tai toisella. Samalla kun biljoonat laitteet kommunikoivat keskenään ja keräävät dataa, niin jotkut osapuolet iskevät sieltä mistä ns. turvallisuusaita on matalin. (Lindstedt 2015, 1-2.)

Käytännössä kaikki mikä on yhteydessä Internetiin, on periaatteessa hakkeroitavissa. Esimerkiksi netin kautta voi halutessaan seurata hakkeroitujen valvontakameroiden reaaliaikaista videokuvaa sekä julkisista että yksityisistä tiloista asianosaisten tietämättä. Riskit ovat valtavia, kun kriittisiin kohteisiin liitetyt laitteet ovat yhteydessä nettiin. Mitä vahinkoa voisikaan sattua kun nettirikolliset iskevät hampaansa energiatuotannon ja lääketieteen laitteisiin tai lentolaitteisiin ja ajoneuvoihin. Epäilijät painottavat varovaisuutta, kun siirrytään kohti näitä järjestelmiä ja sovelluksia. (Lindstedt 2015, 2.)

Mihin kaikki kerätty tieto tallennetaan, jos tietoa kerätään tulevaisuudessa jopa sadoista miljardeista eri pisteistä? IoT –kehityksen asettamat vaatimukset nykyisille tieto- ja viestintäjärjestelmille ovat kovat, mutta tästä huolimatta standardeja luodaan IoT –buumin myötä hurjaa tahtia eri puolilla maailmaa. (Lindstedt 2015, 2.)

Jokapäiväiset hakkerointi -hyökkäykset tulevat yleistymään eikä yksikään organisaatio ole näille immuuni. On syytäkin olla huolestunut tai jopa peloissaan siitä miten helppoa tiedon varastaminen on etenkin nopeasti kasvavassa ja yhdistyvässä Internet of Everything:ssä. Professori Pentland Massachusetsin Instituutista (MIT) on esittänyt muutaman varteenotettavan idean, joilla voitaisiin kehittää turvallisuutta ja yksityisyyttä. Sen sijaan, että yhtiöt (esim. Facebook ja Twitter) omistavat syöttämääsi ja luomaasi tietoa itsestäsi, niin olisit laillisesti kaiken itseen kuuluvan tiedon omistaja. Harvemmin käyttäjät lukevat turvallisuusehtoja ja esimerkiksi Facebook:sta tulee välittömästi lataamasi kuvan omistaja. Jos selkeys tiedon omistajuudesta saataisiin liikkeeseen niin henkilökohtaisesta informaatiosta tulisi valuuttaa. Näin kaikki suhteellisen typerä data, joka liikkuu Internetissä saisi älykkäämmän muodon. Tästä seuraisi myös tarkempi lakien ja menettelytapojen valvominen. Tietopankit hyödyntäisivät myös meitä, kun puhutaan oman tiedon omistajuudesta. Olisimme oikeutettuja saamaan joko rahallinen tai vastaava korvaus siitä, että jokin yritys haluaisi käyttää meidän henkilökohtaisia preferenssejä. Tutkimusyhtiö Ctrl-Shift:in mukaan useita vastaavanlaisia tietopankki –palveluja on jo olemassa. (Evans 2013, 1-2.)

Tieto on arvokasta. Tästä syystä turvallisuus ja yksityisyyskysymykset ovat vakavasti otettavia asioita. Tietoturvayritys Proofpoint raportoi ensimmäistä laatuaan olevasta verkkohyökkäyksestä, joka on toteutettu IoT:n avulla. Hyökkäyksessä käytettiin hyväksi yli 100 000 kotikäyttöistä laitetta, kuten reitittimiä, multimediakeskuksia, televisioita ja yhtä jääkaappia. Näiden avulla lähetettiin yli 750 000 roskapostia. Kyseinen hyökkäys tapahtui joulukuun 2013 ja tammikuun 2014 välillä. Esineiden Internetllä on mahdollisuus yhdistää suuri määrä kotikäyttöisiä laitteita, mutta tämä tulee houkuttelemaan kyberhyökkääjiä toimimaan, koska näiden suojaukset ovat helposti murrettavissa. Useassa tapauksessa laitteisiin päästään käsiksi, koska ne ovat väärin asennettu. (Marketwatch 2014, 1-2.)

Toinen tietoturvayritys Veracode otti testattavakseen muutaman IoT –laitteen seurattakseen sen datan siirtoa ja mitä turvallisuusvuotoja näissä ilmenee. Yhtiön mukaan useammista löytyi merkittäviä heikkouksia eikä turvallisuuteen ja yksityisyyteen oltu keskitytty tarpeeksi. Näin kuluttajat joutuvat helpommin hyökkäysten kohteeksi. (Hesseldahl 2015, 1-2.)

Yksi kohde oli MyQ -autotallin testaus, jossa käyttäjä voi älypuhelimella avata ja sulkea autotallin oven. Veracoden mukaan varas kykeni murtautumaan systeemiin ottaen selville milloin ovi on avattu ja suljettu, joka avasi mahdollisuuden murtautua taloon. (Hesseldahl 2015, 1-2.)

Toinen laite oli Wink Relay, joka toimii kosketusnäytöllä esimerkiksi valokatkaisijan vieressä ja sillä voi kontrolloida talon muita älylaitteita. Laite toimii Googlen Android –käyttöjärjestelmällä. Veracoden mukaan se pystyi hyödyntää Android Debug Bridgeä (ADB), jota ohjelmoijat käyttävät käyttöjärjestelmän koodin ongelmanratkaisuun. Veracode pystyi käyttää ADB:tä aktivoidakseen laitteen mikrofonin, nauhoittaa keskusteluja ja ladata näitä tietokoneelle. (Hesseldahl 2015, 1-2.)

Vähiten turvallisuuteen liittyviä ongelmia ilmeni SmartThings Hub:ssa, joka yhdistää sensoreita, lukkoja, valokatkaisijoita, termostaatteja ja muita talon sisäisiä älylaitteita. SmartThings Hub toimii Telnet –serverillä ja siinä olisi mahdollisuus avata hyökkääjille pääsy järjestelmään, mutta Veracoden insinöörit eivät onnistuneet murtautumaan siihen. On selvää, että laitteiden arkkitehtuuriin ja sovelluksiin on tehtävä parannuksia koskien turvallisuutta. (Hesseldahl 2015, 1-2.)

9 Yhteenveto

Tämän opinnäytetyön tarkoituksena oli perehtyä esineiden Internetissä käytettäviin standardeihin ja protokolliin sekä niitä sivuaviin käsitteisiin ja ratkaisujen toimivuuteen. IoT tulee olemaan selkeästi yksi suurimmista ilmiöistä sitten älypuhelimien nousun jälkeen. Vielä 10 vuotta sitten kämmenen kokoinen älypuhelin tuntui hämmentävältä, mutta muutaman vuoden päästä nykyhetkestä jokaista ihmistä tulee ympäröimään kymmenistä satoihin sensoria tai laitetta, jotka keräävät dataa ympärillä tapahtuvista asioista. Selvää on, että ajan kanssa toimijoita tulee huomattavasti lisää IoT:n potentiaalin takia. Toiset ottavat osaa rahallisen hyödyn takia, mutta monet haluavat viedä yhteiskuntaa eteenpäin samalla parantaen ihmisten ja laitteiden välistä kommunikointia. IoT –laitteita tulee olemaan tulevaisuudessa niin valtaisa määrä, että IPv4:sta siirtyminen IPv6:seen alkoi juuri oikeaan aikaan.

Bluetooth, ZigBee ja Wifi ovat selkeästi suosituimmat tavat yhdistää päätelaitteet keskenään. Nämä toki jatkavat taisteluaan markkinoilla kehittäen uusia ratkaisuja. ZigBeen suurimpana etuna on Mesh –topologian käyttöominaisuus, joka on usein käytännöllisempi langattomissa verkoissa, mutta Bluetooth on tuomassa saman ominaisuuden uusiin versioihin. Verrattaessa WiFi:n ja Bluetooth:in ominaisuuksia, voidaan todeta WiFi:n olevan edellä esimerkiksi tietoturvassa ja nopeudessa. Bluetooth on kehittänyt laajentaakseen toimintasädettä ja molempien kantavuus on noin 30 metrin luokkaa. Bluetooth:in eduksi voidaan lukea sen helppokäyttöisyyden ja toimivuuden useamman laitteen kanssa samanaikaisesti. WiFi sen sijaan vaatii laitteiston asennuksen ja ohjelmiston. Juuri tästä syystä voidaan Bluetooth:in nähdä olevan muita vahvempi IoT –markkinoilla. Toki huomioon täytyy ottaa myös käyttökohteen tarkoitus, jotta siitä saadaan paras hyöty irti.

Maailman johtavat teknologiayritykset yhdistyvät kehittelemään uusia standardeja, joilla saadaan laitteet kommunikoimaan keskenään ja toimimaan sulavasti näiden ohjaamien applikaatioiden kanssa. Standardeja on paljon ja niissä määritellään metodit, prosessit, toimenpiteet ja protokollat. Avoimen standardin liittoutumat kehittävät ratkaisujaan eri teollisuuden, kuten terveys- ja energia-alalle tavoitteenaan luoda kustannuksia ja energiaa säästävä ympäristö. Lisäksi tavoitteena on kehittää kuluttajille ehkä tärkeämpiä IoT -ratkaisuja, kuten kodin turvallisuus ja mukavuus.

Jatkuvasti kehittyvä teknologia tulee vaikuttamaan suuresti sekä yksityishenkilöiden että yritysmaailman tapoihin toimia jokapäiväisessä elämässä. Vielä noin vuosikymmen sitten markkinoille tuotiin ensimmäisiä älypuhelimia ja tabletteja. Hyvin nopean kehityksen joh-

dosta jo nyt näitä laitteita pystytään hyödyntämään aistimaan ympäristöä, keräämään dataa ja tallentamaan kaiken prosessointia varten. Vaativampaa onkin saada laitteet toimimaan saumattomasti keskenään keräten valtavan määrän jatkuvasti virtaavaa dataa ilman ihmisen puuttumista prosessiin. IoT:n tarkoituksena onkin mullistaa koko tieto- ja viestintäteollisuus ja viedä langaton nettiliikenne aivan uudelle tasolle. Lisäksi tarkoitus on integroida IoT osaksi 5G –järjestelmää, jonka povataan yleistyvän ensi vuosikymmenellä.

IoT –laitteet toimivat pääosin paristoilla ja yksi päätavoitteista tulee olemaan näiden mahdollisimman pitkä aika toimia ilman ylimääräisiä latauksia. Riittävä energiatehokkuus on yksi isoimmista haasteista, koska datan keruu ja tallentaminen vaatii laitteilta tehoa. Samat haasteet löytyvät myös älypuhelimista. Monia IoT –laitteita ja sensoreita tullaan ohjaamaan juuri älypuhelimissa käytettävien sovellusten kautta ja tämä tulee viemään entistä enemmän virtaa jo nyt suhteellisen vähän aikaa yhtäjaksoisesti toimivilta laitteilta. Tutkijat pyrkivät löytämään ratkaisuja energian tuotantoon. Kehitteillä on uusia tapoja kerätä tehoa esimerkiksi ympäristön radiosignaaleista ja aurinkokennoista, joilla voitaisiin luoda jonkinasteinen tasapaino energiaa tuottavien elementtien tehokkuudessa ja aktiivisten laitteiden energiankulutuksen välillä.

Suurin kysymysmerkki onkin erityisesti tietoturvariskit, jotka tulevat jarruttamaan kehitystä. Vaikka IoT on kehityksensä alkupäässä, niin tähän mennessä on jo tullut raportoituja verkkohyökkäyksiä. Toisaalta on hyvä, että näin on tapahtunut, jotta ei päästä unohtamaan valtavia riskejä mitä IoT –maailmaan tulee liittymään. Jokaisen yksityisyys on entistä uhatumpi, kun henkilökohtainen informaatio liikkuu verkossa laitteiden välityksellä ja IoT:n myötä jopa pidempiä aikavälejä ilman ihmisen puuttumista automatisoituun prosessiin. Tietoturvayritysten teettämät laite- ja sovellustestaukset ovat osoittaneet suuria puutteita turvallisuudessa ja näillä herätetään yritykset ja liittoutumat keskittymään entistä enemmän juurikin turvallisuusasioihin.

9.1 Ajatuksia jatkotutkimuksista

Tämän tutkimuksen aiheen lähtökohtana oli Haaga-Helian antama toimeksianto selvittää esineiden Internetissä käytettäviä antureita ja päätelaitteita, sekä miten informaatio liikkuu verkon välityksellä näiden laitteiden välillä. Haaga-Helian kehityshankkeen tavoitteena on perustaa koulun tiloihin oma demoympäristö ja tämä tutkimus toimii yhtenä tietopohjana tälle hankkeelle.

Useammat toimijat IoT -alalla ovat hyvin optimistisia ja toiveikkaita omien ratkaisuiden ylivertaisuuteen. Perehtyessä tarkemmin näihin ratkaisuihin ensimmäisenä tulee mieleen

mahdolliset ongelmat, kuten luvuissa 7 ja 8 käsiteltävät IoT:n virranhallintaratkaisut ja tietoturva. Vauhti kehittyä on kova, mutta kuten esimerkiksi älypuhelimien kanssa, kehitys ei mene käsi kädessä laitteiden virranhallinta- ja tietoturva –asioiden kanssa. Tästä aiheesta olisi varmasti hyödyllistä tehdä lisätutkimus, josta olisi merkittävää apua IoT -ratkaisuja kehitteleville yrityksille.

Mielenkiintoista olisi myös tutkia muutaman vuoden kuluessa mitä IoT -ratkaisuja yritykset ovat tuoneet markkinoille. Ajan kuluessa olisi myös konkreettista näyttöä laitteiden toimivuudesta, hyödyllisyydestä ja virranhallinnasta. Tässäkin työssä on tutkittu eri protokollia ja niiden ominaisuuksia, niin olisi kiinnostavaa nähdä tuloksia miten laitteet käytännössä soveltuvat toimimaan niiden pohjalta.

Monet teollisuuden alat tulevat saamaan paljon IoT:n kehityksen myötä. Terveydentilan tarkkailu, kodinkoneiden energiankulutus ja autoilu ovat kaikki varteenotettavia tutkimuksen kohteita. Miten autoilusta saadaan turvallisempaa kun liikennevalot ja nopeustaulut mukautuvat todellisiin liikenneolosuhteisiin tai miten termostaatit ja valaisimet oppivat päivittäisiin rutiineihin esimerkiksi säätämällä kodin lämpötilaa optimaaliselle tasolle? Lukematon määrä kehitystä juurikin liikenteeseen, sairaaloihin ja älykoteihin tuo vastapainona myös suuremmat turvallisuusriskit. Kuka pääsee kontrolloimaan kodin älylaitteita tai voiko joku kontrolloida autoa kesken ajon? Tässä on olemassa riski, kun ottaa käyttöön liian monta itsenään toimivaa laitetta kontrolloimaan itseään ympäröiviä asioita. On hyvin tärkeää tutkia laitteiden ja yhteyksien turvallisuus ennen käyttöönottoa.

9.2 Työprosessi ja oma oppiminen

Ennen tutkimuksen alkua esineiden Internet ei ollut lainkaan tuttu käsite. Hitaanpuoleisen alun jälkeen kokonaiskuva IoT:n maailmasta alkoi hiljalleen muodostua. Alussa oletuksena oli, että kyseessä olisi vasta tulevaisuudessa esiintyvää teknologiaa, kunnes materiaaliin tarkemmin tutustuen ilmeni, että sitä on ollut jo tarjolla ja esillä viimeisten vuosien ajan. Pääosin uutta tekniikkaa näytti tosin olevan vain yritysten mielikuvissa ja tulevaisuuden näkymissä. Haastavampaa olikin löytää ja saada tutkimukseen puolueettomien tahojen näkökantoja IoT –maailmaan. Yritykset näitä näkökantoja eivät tarjoa, mutta onneksi verkosta löytyy paljon tutkijoita, joiden näkökantoihin oli hyvin mielenkiintoista tutustua ja tuoda mukaan tähän työhön. Aiheen rajaus alkoi selkiintymään vasta työn aloittamisen jälkeen, kun aloin ymmärtämään hieman enemmän IoT:n kokonaisuutta.

Työ eteni alun vaikeuksien kautta hyvin, koska työlle oli asetettu takaraja. Vaatimuksena oli saattaa työ loppuun kevätlukukauden (2015) aikana. Koin tämän suhteellisen realisti-

seksi tavoitteeksi vaikka projekti lähti varsinaisesti käyntiin vasta myöhemmin keväällä. Suurimpana huolenaiheena heti projektin alkumetreillä oli se, että löytyisikö aiheesta riittävästi taustamateriaalia. Vaikka kyseessä on suhteellisen tuore aihepiiri, ongelmaksi muodostui enemmänkin se, että lähteitä oli tullut kerättyä jopa hieman liikaa. Hyvä puoli valtaosassa käyttämistäni lähteistä oli niiden ajankohtaisuus. Pyrin enemmänkin juuri käyttämään lähteitä, joissa käsiteltiin IoT –aihetta puolueettomasti. Lähteistä oli tärkeä saada karsittua mainostava ja tiettyjä toimijoita suosiva sisältö. Näin sain mielestäni riittävän objektiivisen kirjallisuuskatsauksen.

Ottaen huomioon lähtökohdat, jossa tietopohjani aiheeseen oli hyvin rajoittunut, asiantuntemus ja ymmärrys esineiden Internetiä koskevaan maailmaan laajenivat työn myötä huomattavasti. Opinnäytetyö ja aiheeseen perehtyminen on myös herättänyt kiinnostuksen jatkaa alan kehityksen seuraamista.

Aineiston käsittelyn ja rajauksen suhteen kokemus oli hyvin opettava ja mielenkiintoinen. Omien vahvuuksien ja heikkouksien tunnistaminen on ollut tärkeä osa työn edetessä. Viimeisen kymmenen vuotta olen keskittynyt työssäni hyvin pitkälti käytännön tekemiseen, joka on lähes täysi vastakohta opinnäytetyön kirjallisen aineiston tutkimiseen ja keräämiseen. Vaikka kokemusta työelämästä on karttunut useampi vuosi sekä työntekijänä että yrittäjänä, niin jatkossa osaan kiinnittää entistä enemmän huomiota niihin osa-alueisiin, joissa koen olevan jotain parannettavaa.

Lähteet

AllSeen Alliance Data Sheet 2015. Luettavissa: https://allseenalliance.org/sites/default/files/resources/AllSeen-Alliance-DataSheet-English-021015.pdf. Luettu 16.3.2015

AllSeen Alliance FAQs 2015. Luettavissa: https://allseenalliance.org/about/faqs#faq29. Luettu 16.3.2015

Ashton, K. That 'Internet of Things' Thing. Luettavissa: http://www.rfidjournal.com/articles/view?4986. Luettu 9.3.2015

Barrett, J. 2012. The Internet of Things: Dr. John Barrett at TEDxCIT. Luettavissa: https://www.youtube.com/watch?v=QaTIt1C5R-M. Luettu 23.3.2015

Bartleson, K. 2014. The Internet of Thing Is A Standards Thing. Luettavissa: http://electronicdesign.com/communications/internet-things-standards-thing. Luettu 24.3.2015

Bluetooth.com 2015. Luettu 12.3.2015. Luettavissa: http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx. Luettu 12.3.2015

Cisco 2014. Attaining IoT Value: How To Move from Connection Things to Capturing Insights. Luettavissa: http://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/data-analytics/iot-whitepaper.pdf. Luettu 20.3.2015

Cisco / IoTWF 2014. The Internet of Things Worl Forum Unites Industry Leaders in Chicago to Accelerate the Adoption of IoT Business Models. Luettavissa: http://diaryofthings.com/internet-things-world-forum-unites-industry-leaders-chicago-accelerate-adoption-iot-business-models/ Luettu 4.5.2015

Elahi, A., Gschwender, A. 2009. Introduction to the ZigBee Wireless Senso and Control Network. Luettavissa: http://www.informit.com/articles/article.aspx?p=1409785&seqNum=4. Luettu 30.3.2015

Etn 2015. Wifi ja Bluetooth sovussa samalla sirulla. Luettavissa:

http://etn.fi/index.php?option=com_content&view=article&id=2580%3Awifi-ja-bluetooth-sovussa-samalla-sirulla&catid=13&Itemid=101. Luettu 25.3.2015

Evans, D. 2013. Answering the Two Most-Asked Questions About the Internet of Everything. Luettavissa:
http://blogs.cisco.com/ioe/answering-the-two-most-asked-questions-about-the-internet-of-everything. Luettu 23.3.2015

Gallagher, S. 2015. New ARM –powered chip aims fo battery life measured in decades. Luettavissa:
http://arstechnica.com/information-technology/2015/03/30/new-arm-powered-chip-aims-for-battery-life-measured-in-decades/. Luettu 6.5.2015

Gigaom 2014. Samsung claims a WiGig breakthrough that promises multi-gigabit wireless speeds. Luettavissa:
https://gigaom.com/2014/10/13/samsung-claims-a-wigig-breakthrough-that-promises-multi-gigabit-wireless-speeds/. Luettu 25.3.2015

Hesseldahl, A. 2015. A Hacker's-Eye View of the Internet of Things. Luettavissa:
http://recode.net/2015/04/07/a-hackers-eye-view-of-the-internet-of-things/
Luettu 5.5.2015

ICPDAS-USA 2015. ZigBee Introduction. Luettavissa:
http://www.icpdas-usa.com/zigbeeintro.php. Luettu 30.3.2015

IEEE 2015. P2413 – Standard for an Architectural Framework for the Internet of Things (IoT). Luettavissa:
http://standards.ieee.org/develop/project/2413.html
Luettu: 15.4.2015

IETF 2015. About the IETF. Luettavissa:
https://www.ietf.org/about/. Luettu 31.3.2015

Industrial Internet Consortium 2015. Luettavissa:
http://www.iiconsortium.org/about-us.htm. Luettu 20.3.2015

Intel 2014. Intel IoT – What Does The Internet of Things Mean? Luettavissa:
https://www.youtube.com/watch?v=Q3ur8wzzhBU. Luettu 9.3.2015

IoT Awards 2015. Luettavissa:
http://postscapes.com/internet-of-things-award/2014/. Luettu 16.3.2015

Iot6.eu. IPv6 for IoT. Luettavissa: http://iot6.eu/ipv6_for_iot
Luettu 10.4.2015

Jäntti, J. 2014. Samsungilta tulossa Wi-Fi-laitteita yli 500 Mt/s tiedonsiirtonopeudella. Luettavissa:
http://muropaketti.com/samsungilta-tulossa-wi-fi-laitteita-yli-500-mts-tiedonsiirtonopeuksilla. Luettu 25.3.2015

Laitila, T. 2015. Esineiden internet saattaa viestiä langattomasti ilman sähköä. Luettavissa:
http://www.mpc.fi/kaikki_uutiset/esineiden+internet+saattaa+viestia+langattomasti+ilman+sahkoa/a1001711?service=mobile. Luettu 25.3.2015

Lattice 2015. Energy Efficiency: The Common Denominator in the Internet of Things. Luettavissa:
http://www.latticesemi.com/~/media/Documents/WhitePapers/HM/LatticeSemiconductorIoTWhitePaper.pdf?document_id=50985
Luettu 15.4.2015

Lawson, S. 2014. Why Internet of Things 'standards' got more confusing in 2014. Luettavissa:
http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html. Luettu 20.3.2015

Lawson, S. 2015. Bluetooth starts weaving its mesh for IoT. Luettavissa:
http://www.pcworld.com/article/2888596/bluetooth-starts-weaving-its-mesh-for-iot.html.
Luettu 31.3.2015

Lindstedt, S. 2015. Visioissa: Esineiden Internet. Luettavissa:
http://www.mbnet.fi/artikkeli/ajankohtaiset/visioissa_esineiden_internet. Luettu 30.3.2015

Linux Foundation 215. Luettavissa:
http://www.linuxfoundation.org/. Luettu 16.3.2015

Marketwatch 2014. Proofpoint Uncovers Internet of Things Cyberattack. Luettavissa: http://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16?reflink=MW_news_stmp. Luettu 23.3.2015

Merilinna, J. Tietoliikenteen perusteet. Luettavissa: http://hhmoodle.haaga-helia.fi/pluginfile.php/412065/mod_resource/content/1/Tietoliikenteen%20perusteet.pdf Luettu 24.4.2015

Mouser 2015. Atmel WINC1500 Wi-Fi System on Chip. Luettavissa: http://fi.mouser.com/new/atmel/atmel-winc1500/. Luettu 25.3.2015

Open Interconnect Consortium 2015. Luettavissa: http://openinterconnect.org/. Luettu 18.3.2015

Polar 2015. Luettavissa: http://www.polar.com/fi/. Luettu 16.3.2015. Luettu 16.3.2015

Reiter, G. Wireless connectivity for the Internet of Things. Luettavissa: http://www.ti.com.cn/cn/lit/wp/swry010/swry010.pdf. Luettu 12.3.2015

Rouse, M. 2015. Metropolitan area network. Luettavissa: http://searchnetworking.techtarget.com/definition/metropolitan-area-network-MAN Luettu 16.3.2015

Rouse, M. 2015. IPv6. Luettavissa: http://searchenterprisewan.techtarget.com/definition/IPv6. Luettu 16.3.2015

Saroj, K. 2015. Luettavissa: http://cloudtimes.org/2015/01/21/intel-samsung-cisco-launches-iotivity-open-source-standard-for-the-internet-of-things/. Luettu 16.3.2015

Shelby, Z. 2014. Constrained Application Protocol (CoAP) Tutorial. Luettavissa: https://www.youtube.com/watch?v=4bSr5x5gKvA. Luettu 3.4.2015

Schneider, S. 2014. Understanding The Protocols Behind The Internet Of Things. Luettavissa:

http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things#Protocol%20Overview. Luettu 17.3.2015

Suomen Standardisoimisliitto 2014. Esineiden Internetin viitearkkitehtuurista standardi. Luettavissa: http://www.sfs.fi/standardien_laadinta/sfs_n_tekniset_komiteat_ja_seurantaryhmat/it-standardisointi/it_-_ajankohtaista/it-uutisarkisto/esineiden_internetin_viitearkkitehtuurista_standardi.2020.news. Luettu 24.3.2015

Sutaria, R., Govindachari, R. 2013. Understanding The Internet Of Things. Luettavissa: http://electronicdesign.com/communications/understanding-internet-things#IoT. Luettu 26.3.2015

Syrjälahti, M. 2015. Härveleiden Internet. Luettavissa: http://ibisense.com/wp-content/uploads/2014/08/Automaativayla_3_2014_sivut25_27.pdf. Luettu 1.4.2015

Thread Group 2015. Luettavissa: http://www.threadgroup.org/About.aspx. Luettu 20.3.2015

UKessays 2015. Origin Of Name Zigbee Information Technology Essay. Luettavissa: http://www.ukessays.com/essays/information-technology/origin-of-name-zigbee-information-technology-essay.php. Luettu 27.3.2015

Verizon 2015. Luettavissa: http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf. Luettu 16.3.2015

WiFi Alliance 2015. Discover Wi-Fi 15 Years of Wi-Fi. Luettavissa: http://www.wi-fi.org/discover-wi-fi/15-years-of-wi-fi. Luettu 27.3.2015

ZigBee Alliance 2015. Luettavissa: http://www.zigbee.org/. Luettu 27.3.2015

Z-Wave Alliance 2015. Z-Wave Alliance Launches IoT Competition to Reward Start-Ups for Their Innovation in the Smart Home. Luettavissa: http://finance.yahoo.com/news/z-wave-alliance-launches-iot-170000838.html Luettu 4.5.2015